UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Análisis de Riesgos de los activos de Información del proceso de Contratación de Personal Docente en la Dirección Regional de Educación basado en las directrices de la ISO/IEC 27005.

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR(A): CHUNGA

RAMIREZ KATIA

ASESOR:

MG. QUITO RODRIGUEZ CARMEN ZULEMA

LINEA DE INVESTIGACIÓN:

AUDITORÍA DE SISTEMAS Y SEGURIDAD DE INFORMACIÓN

Piura - Perú

2017

DEDICATORIA

Esta investigación está dedicada a mi “Creador” y a toda mi familia que me ayudó en este proceso y sobre todo a mi madre Marleni y a mi padre Lucio en conjunto con mis hermanos Jacqueline, Kelwin, Jens, Juan y Alfredo que me dan su amor y apoyo incondicional a lo largo de mi vida, por todo el tiempo y confianza que han tenido en mí.

AGRADECIMIENTO

A mis profesores de la Escuela de Ingeniería de Sistemas que han aportado mucho en mis conocimientos y actitudes hacia esta grandiosa carrera.

A la Abogada Doris Alberca Ríos, por brindarme su apoyo para realizar la investigación en la DRE Piura.

Al Ing. Luis. A Torres Preciado, por ayudarme y brindarme información para desarrollar esta investigación.

A la Alta Dirección de la DRE Piura, por brindarme la información para desarrollar esta investigación.

PRESENTACIÓN

La presente investigación, fue llevada a cabo con el propósito de analizar los riesgos de los activos de Información del proceso de Contratación de Personal Docente en la Dirección Regional de Educación basada en las directrices de la ISO/IEC 27005. Este estudio está estructurado en siete capítulos, los cuales se detallan a continuación:

En el capítulo I se presenta la realidad problemática donde se inicia la investigación, conocer en qué teorías se ha basado y otros trabajos previos que sirven de apoyo para esta tesis, así como los objetivos que se desean lograr. En el capítulo II, se menciona la metodología empleada para llevar a cabo la investigación, la variable que interviene, cual es el proceso de estudio y que técnicas e instrumentos que permitieron recoger información.

El capítulo III, se presenta los resultados de la investigación, siguiendo las dimensiones de la variable de estudio. El capítulo IV, se discuten los resultados de la investigación con las teorías y antecedentes presentados.

Por otra parte el capítulo V se sitúan las conclusiones a las que se llegó luego de realizar todo el proceso de investigación, para dar lugar a las recomendacion es descritas en el capítulo VI, son ideas de otras investigaciones teniendo en cuenta este estudio, para el planteamiento de nuevos problemas que se pueden desarrollar para nuevas investigaciones.

Y por último VII se presenta la propuesta, las políticas de seguridad y los controles correctivos y preventivos, la misma que pretende ayudar a la DREP a mitigar los riesgos de los activos de información del proceso contracción de personal Docente, que están presentes en la organización.

La autora.

ÍNDICE GENERAL

RESUMEN

Análisis de riesgos de los activos de información del proceso de Contratación de Personal Docente en la Dirección Regional de Educación de Piura basada en las directrices del ISO/IEC 27005 - Katia Chunga Ramírez.

La presente investigación tiene como objetivo evaluar los riesgos de los activos de información que intervienen en el proceso de contratación de personal docente en la DREP basado en las directrices del ISO/IEC 27005, ya que los altos directivos no conocen de forma clara los riesgos a la que está expuesta la organización.

Esta investigación toma como punto de partida el estudio de la norma ISO/IEC 27005 para el desarrollo del análisis de riesgo que permitirá evaluar los activos de información basándose en las siguientes etapas; definición de alcance, identificación de activos de información, clasificándolos según su tipología, para luego valorar cada activo, teniendo en cuenta las tres propiedades bases del SGSI (sistema de gestión de la seguridad de la información)como son la confidencialidad, la integridad y la disponibilidad; después se identifican los riesgos y amenazas que son más vulnerables con el fin de determinar la probabilidad e impacto que tendría la organización, dando como resultado el nivel de riesgo.

Por último se propuso controles que permitan mitigar o reducir los riesgos identificados.

Para el desarrollo de la investigación se utilizaron instrumentos como guías de observación, cuestionarios y entrevistas, debidamente validadas.

Como resultados del análisis de riesgos se muestra que un 34% de activos de información que se identificaron en el proceso de contratación de personal docente de la DREP tienen una Alta criticidad.

Palabras claves: Análisis de riesgos de activos de información, ISO/IEC 27005, riesgo, activos de información.

ABSTRACT

Risk analysis of the information assets of the Process of Recruitment of Teaching Personnel in the Regional Direction of Education of Piura based on the guidelines of ISO / IEC 27005 - Katia Chunga Ramirez.

The present research aims to evaluate the risks of the information assets involved in the recruitment of teachers in the DREP based on the guidelines of ISO / IEC 27005, since senior managers do not know clearly the risks to Which is subject to the organization.

This research takes as its starting point the study of the ISO / IEC 27005 standard for the development of the risk analysis that will allow to evaluate the information assets based on the following stages; Definition of scope, identification of information assets, classifying them according to their typology, and then valuing each asset, taking into account the three basic properties of the ISMS (information security management system) such as confidentiality, integrity and availability; Then identify the risks and threats that are most vulnerable in order to determine the likelihood and impact that the organization would have, resulting in the level of risk.

Finally, controls were proposed to mitigate or reduce identified risks. For the development of the research instruments were used as guides of observation, questionnaires and records duly validated.

As results of the risk analysis shows that 34% of information assets that were identified in the recruitment process of teachers of the DREP have a high criticality.

Keywords: Risk analysis of information assets, ISO / IEC 27005, risk, information assets.

I.INTRODUCCIÓN

1.1 Realidad problemática

La creciente necesidad de las organizaciones de implementar proyectos de seguridad de la información, surge porque toda entidad se sustenta a partir de la información referente a sus procesos, independientemente de su medio de almacenamiento y transmisión; es por eso que se debe proteger frente a riesgos y amenazas para asegurar el correcto funcionamiento de las organizaciones y por ende de sus procesos.

Los riesgos del funcionamiento para las entidades públicas en todos sus procesos cobran hoy mayor importancia, dado el dinamismo y los constantes cambios del mundo globalizado que hoy existe.

La Dirección Regional de Educación de Piura (en adelante DREP) es una entidad gubernamental que permite instanciar la gestión educativa descentralizada; rectora de la educación de Piura que promueve y asegura el servicio educativo en la región, y para el cumplimiento de sus funciones, en la DREP están asistidos por activos de información.

Un proceso importante para la DREP es la contratación de personal Docente, ya que en dicho proceso se maneja información de todo el personal contratado que previamente ha sido seleccionado por una UGEL (Unidad de Gestión Educativa Local) para luego formalizar el contrato asignándole la plaza a la que se ha postulado.

En este proceso son asistidos por activos de información, los cuales se pueden clasificar en sistemas, aplicaciones, servicios, redes, personal, tecnologías usadas para procesar, almacenar y comunicar información.

El problema principal es que no administran sus riesgos, ya que los incidentes que ocurren es cuando recién ponen manos a la obra, y no se toman medidas preventivas o correctivas, es por eso que las amenazas y vulnerabilidades que se suscitan se deben registrar y tener en cuenta que medidas o controles se deben tomar en cuenta, para que el personal en general sepa que hay una gran probabilidad e impacto que afecte a la institución.

Muchos problemas se pueden suscitar ya que estos activos están disponibles en ambientes sin tomar medidas de seguridad, cada vez interconectados por amenazas y vulnerabilidades. Como pueden ser amenazas de tipo natural, como es la lluvia y calor, que la ciudad de Piura, casi la mayoría de tiempo es su clima, en todo caso no se toman en cuenta este tipo de amenas para las instalaciones de la DREP, no registran incidentes de años pasados, lo cual también pueden incrementarse aún más gracias a las vulnerabilidades a las que los mismos funcionarios pueden cometer como por ejemplo dejar los libros de cargos en una simple percha sin tomar medidas de protección.

Los problemas anteriores deben ser corregidos o minimizados; una institución no puede operar de manera eficiente bajo estas condiciones sin tomar precauciones, sobre todo deben tener en cuenta a qué amenazas y vulnerabilidades están expuestas los activos de información, para ello existen estándares que brindan las pautas necesarias para mantener la eficiencia de las operaciones asegurando la información, aunque esto realmente necesita un plan de inversión en seguridad de la información, lo cual se ve que la DREP no está realmente comprometida en este tipo de planes ya que no le dan prioridad.

Para esto se deben identificar y evaluar los riesgos a los que estos están expuestos los activos, mediante las normas internacionales se hace posible la detección de fallas ya que proporcionan controles y técnicas que permiten el análisis de los riesgos de los activos de información.

1.2 Trabajos previos

La tesis de Moncayo (2014), titulada "**Modelo de evaluación de riesgos de Tic's de pequeñas y medianas empresas del sector automotriz**", con el fin de optar el grado de magister en gestión de comunicaciones y tecnologías de la información en la Escuela Politécnica Nacional de Quito. El trabajo de tesis consistió en la creación de un modelo de evaluación de riesgos, basado en las Metodologías Magerit, Octave y normas NIIF (Normas Internacionales de Información Financiera), el mismo que aporto a las empresas a obtener información sobre riesgos, amenazas y protecciones que deben considerar para evitar y tomar medidas de prevención oportunas y adecuadas. Con el objetivo principal que sea un modelo de fácil aplicación ya que ayudó a las organizaciones a dirigir y gestionar las evaluaciones de riesgos por si solos, tomando las mejores decisiones para mitigar y controlar los riesgos. Para la aplicación del modelo fue de tipo cuantitativo y cualitativo, ya que se aplicó una encuesta a los participantes de las empresas en estudio, teniendo acceso a documentación que permitió conocer la situación actual referente a la infraestructura, equipamiento y activos de Tic's.

La tesis de Aliaga (2014), titulada "**Diseño de un Sistema de Gestión de Seguridad de Información para un instituto educativo**", con el fin de optar el título de Ingeniero Informático en la Pontificia Universidad Católica del Perú. El trabajo de investigación consistió en la creación de un SGSI, realizando el previo análisis de riesgos para así emitir controles según el ISO/IEC 27002 a los activos que se encuentren en un nivel de riesgo "ALTO".

El proyecto brinda como alternativa el diseño de un sistema de seguridad de Información para una institución educativa de nivel superior, tomando la realidad de una entidad local, se enfoca en proteger la información de los procesos principales de esta institución educativa siguiendo las normas internacionales vigentes. Con el objetivo de diseñar un sistema de Gestión de Seguridad de Información (SGSI) basado en las normas internacionales ISO/IEC 27001:2005 e ISO/IEC 27002:2005, adoptando como framework de negocios la actual versión de COBIT, modelando sus procesos de negocio que componen el alcance del SGSI establecido por la entidad, así como identificar y valorar los activos de in formación asociados a los procesos del negocio; luego

se identificó, analizó y evaluó los riesgos existentes que se exponen los activos de mayor valor para la institución para que luego se seleccione los controles que les permita gestionar y tratar los riesgos identificados y finalmente se formaliza la aplicabilidad del SGSI con la documentación exigida por la norma internacional adoptada para el diseño del SGSI. Se concluyó que el sistema de gestión de seguridad de información (SGSI) fue una muestra como solución para el flujo de información que se dio en procesos críticos y los activos involucrados dentro de dichos procesos así logro un nivel de seguridad adecuado para garantizar el cumplimiento de los objetivos de TI y, en consecuencia, los objetivos organizacionales.

La tesis de Aguirre (2014), titulada "**Diseño De Un Sistema De Gestión De Seguridad De Información Para Servicios Postales**", con motivo de optar por el Título de Ingeniero informático en la Pontificia Universidad Católica del Perú, se presentó en la ciudad de Lima - Perú. El trabajo de investigación se basó en la fase de planificación de in Sistema de Gestión de Seguridad de la Información basado en la NTP ISO/IEC 27001:2008 y la NTP ISO/IEC 17999:2007, para una institución pública en este caso a SERPOST. Su objetivo de la investigación fue diseñar un sistema de gestión de seguridad de información para SERPOST según lo indicado por la NTP ISO/IEC 27001:2008 y la NTP-ISO/IEC 17799:2007 de la seguridad de la información. Tuvieron como objetivos la elaboración de la documentación exigida por la NTP ISO/IEC 27001 como marco de referencia de seguridad de la información para la organización, para luego valorar los activos de información más importantes y ser objetivo de un análisis de riesgos siguiendo con el cronograma de implementación incremental propuesto por la ONGEI y por ultimo finali zar una lista de controles a implementar en la organización, con ese documento la organización termino la fase II del cronograma de implementación incremental y para luego empezar con la fase de despliegue. Se concluyó que el apoyo de la alta gerencia para el diseño de este sistema de gestión fue preciso, debido a que fue necesaria su intervención para ayudar a concientizar a los jefes de área y dueños de los procesos a participar de las entrevistas de levantamiento de información y ayudó a que entendieran que el SGSI no solo busca proteger la información digital, sino toda la información crítica del negocio independientemente del medio que la contenga.

1.3 Teorías relacionadas al tema

El estándar internacional ISO/IEC 27005:2008, nos define las directrices para elaborar el proceso de análisis de riesgos, dando soporte particularmente a los requerimientos de un SGSI, de acuerdo con la norma ISO/IEC 27001. Sin embargo, esta norma no es de por sí una metodología para la gestión de riesgos, aunque lo puede llegar a ser según el alcance que el SGSI tenga o el contexto de la gestión de riesgos donde se aplique dicha norma. Teniendo en cuenta los términos básicos como son:

Riesgo

Un riesgo es cualquier evento o circunstancias que de ocurrir amenazarían los objetivos de la organización, estos riesgos tienen una posibilidad de ocurrencia por lo que se miden como la multiplicación de impacto por probabilidad. (ISO/IEC 27005,2008)

Administrar Riesgos

Es el uso de la información para estimar el impacto de los riesgos e identificar sus causas, de esta manera se pueden tomar medidas anticipadas ante un incidente. (ISO/IEC 27005,2008).

Análisis del Riesgo.

Para Alexander (2007) el objetivo del análisis de riesgos es identificar los riesgos basados en la identificación de los activos, de sus amenazas y vulnerabilidades.

El análisis de riesgos puede ser iterativo para la evaluación de los riesgos y/o las actividades que envuelvan el tratamiento de los mismos. Este enfoque iterativo que propone la norma nos puede incrementar la profundidad y el detalle en la evaluación de los riesgos en cada iteración, así como un balance adecuado entre minimizar el tiempo y el esfuerzo en identificar controles adecuados y asegurar que los riesgos con alto impacto y/o posibilidad de ocurrencia estén debidamente monitoreados.

Para analizar los riesgos de los activos de información de la DREP, tratando de llevar a cabo un análisis más detallado sobre el manejo de sus activos, a fin de evaluar los posibles riesgos para poder tomar medidas de acción sobre ellos. Consta de las siguientes etapas:

La integración de las directrices para el análisis de riesgos de la ISO/IEC 27005, a continuación se muestra gráficamente el proceso de integración, a través de la estructura que se desarrollan en la metodología de análisis de riesgos. Para resumir las amenazas deducen vulnerabilidades a los que están expuestos los activos, los mismos que generan impactos y ocasionan riesgos, pero con los debidos Controles y toma de decisiones correctas se puede reducir el riesgo y las vulnerabilidades a los que se exponen los activos de la organización.

Después de revisar las directrices del ISO/IEC 27005 y los diferentes métodos, y herramientas existentes, se propone el esquema que se puede observar en la Figura 1 para llevar a cabo el mencionado análisis de riesgo.

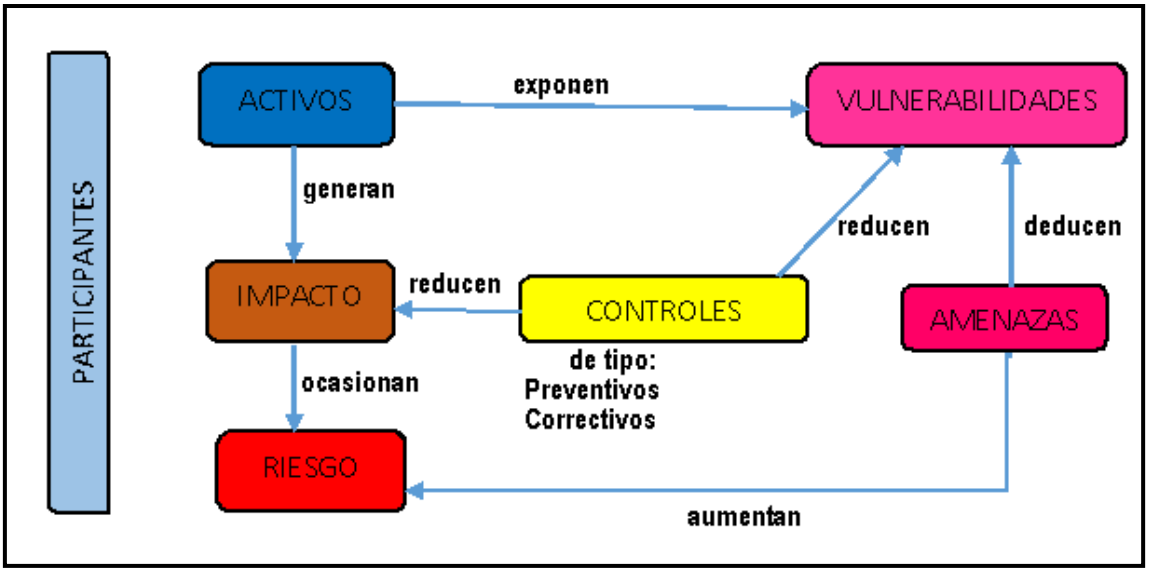


Figura N° 1: Esquema del Análisis de Riesgos.
Elaboración propia

A continuación se describe a detalle la integración, mediante la integración de las siguientes etapas, las mismas que se muestran en la figura.

a) Definición del alcance del modelo.

b) Identificación de activos.
c) Establecer las dimensiones de valoración de los activos.
d) Identificar Amenazas.
e) Determinar la probabilidad e impacto.
f) Identificar controles.

a) Definición del alcance

Según la ISO/IEC 27005 (2008) se trabaja sobre procesos teniendo en cuenta que esto facilita el entendimiento sobre el funcionamiento de la organización y la definición de las interacciones para identificación de activos y riesgos asociados.

El primer paso es definir el alcance para el análisis de riesgos. El alcance de esta evaluación son los activos que son integrantes en el proceso de Contratación de Personal Docente de la DREP.

Según el Manual de Procedimientos Administrativos (MAPRO,2007) de la DREP para el proceso de ***Contratación de personal Docente*** se reconoció seis áreas fundamentales como son : Área de Tramite Documentario, Área de Personal, Área de Gestión Institucional, Dirección de Administración, Dirección de Asesoría Jurídica y la Dirección Regional de Educación.

Con el objetivo Contratar de acuerdo a los requerimientos establecidos y disposiciones vigentes y haber aprobado el proceso de selección correspondiente. El responsable del proceso es el Director del Área de Personal.

A continuación se podrá describir o detallar este proceso de la DREP:

Área de ***Trámite Documentario*** realiza las siguientes actividades diarias y constantes:

- Recepciona file, revisa, folia, adjunta tramite con un número correlativo de registro o expediente, registra el documento presentado por el usuario y lo deriva al Especialista Administrativo.
- Evalúa, determina su trámite y devuelve al Técnico Administrativo.
- Prepara el cargo y entrega el documento al Área de Personal, previo descargo en el Sistema de Trámite Documentario.

- Prepara cargo y distribuye resolución directoral regional a: Dirección de Gestión Institucional (2), Escalafón (1), Administración de Personal (1), Órgano de Control Institucional (1), Remuneraciones (1), Instituto (1), Interesado (1), Autógrafa (3), Archiva la autógrafa y demás copias sobrantes.

Área de ***Personal*** realiza las siguientes actividades:

- Recepciona, registra, evalúa, determina el contrato y deriva al Técnico Administrativo.
- Recepciona, folia, proyecta Resolución Directoral y entrega al Especialista Administrativo.
- Revisa y visa el proyecto de Resolución Directoral Regional y devuelve.
- Prepara cargo y entrega a Secretaria.

Dirección de Administración realiza las siguientes actividades:

- Recepciona, registra proyecto de RDR y deriva a su Jefatura.
- Revisa y visa el proyecto de resolución y devuelve a la Secretaria.
- Prepara cargo y deriva a la Oficina de Gestión Institucional.

Área de *Gestión Institucional* realiza las siguientes actividades:

- Recepciona, registra y deriva al Técnico Administrativo.
- Recepciona, verifica la existencia de plaza codificada por NEXUS, registra el nombre del Trabajador en el Libro de Control de Ejecución, visa y deriva a su Jefatura.
- Visa el proyecto de resolución y deriva a la Secretaria.
- Prepara cargo y deriva a la Oficina de Asesoría Jurídica.

Dirección de *Asesoría Jurídica* realiza las siguientes actividades:

- Recepciona, registra y deriva a su Jefatura.
- Visa el proyecto de resolución y devuelve a la Secretaria.
- Prepara cargo y deriva a la Alta Dirección

Dirección Regional de Educación realiza las siguientes actividades:

- Recepciona, registra y deriva a su Jefatura.

- Revisa, firma tres (3) copias del proyecto de resolución directoral y devuelve a la Secretaria.
- Sella, prepara cargo y deriva.
- Una vez identificado el proceso de contratación de Personal Docente,

Una vez identificado el proceso de contratación de personal docente, se identifica cada uno de los activos de información que están involucrados en el proceso.

b) Identificación Activos de información

Según la ISO/IEC (Estándar Internacional ISO/IEC27005, 2008) se pueden identificar dos tipos de activos: *los primarios* y los de *soporte*. Los primarios, según el estándar antes mencionado, "*son los procesos e información más sensibles para la organización*". Los activos de soporte, "son los activos que dan el debido soporte a estos activos primarios". Dentro de estas dos agrupaciones, se definieron siete distintos tipos específicos de activos:

1*)* Dato: Es toda aquella información que se genera, envía, recibe y gestionan dentro de la organización. Dentro de este tipo, podemos encontrar distintos documentos que la DREP gestiona dentro de sus procesos.

2) Aplicación: Todo aquel software que se utilice como soporte en los procesos.

3) Personal*:* Son todos los actores que se ven involucrados en el acceso y el manejo de una u otra manera a los activos de información de la organización.

4) Servicio: Son los servicios que alguna área de la organización suministra a otra área o entidades externas a la misma.

5) Tecnología: Es todo el hardware donde se maneje la información y las comunicaciones.

6) Instalación: Es cualquier lugar donde se alojan los activos de información. Este lugar o ambiente puede estar ubicado dentro de la organización tanto como fuera de la misma.

7*)* Equipamiento auxiliar: Son los activos que no se hallan definidos en ninguno de los anteriores tipos.

La obtención de esta información, va ser partida inicial de la identificación y clasificación de los activos de información que son de gran importancia para la organización.

c) Dimensiones de valoración

Las dimensiones de valoración para los activos de información se tomaron en cuenta las tres propiedades bases del sistema de Gestión de seguridad de la información, la confidencialidad, la integridad y la disponibilidad de los activos según la ISO/IEC 27001 (2008). Ya que estos se aplicaran para estimar el riesgo que pueden tener estos activos, dando como resultado.

La ***valoración de un activo*** puede ser cuantitativa (escala en una cantidad numérica) o cualitativa (escala de niveles) como por ejemplo: no aplica, nivel bajo, medio y alto, conocidos todos estos niveles como el *apetito del riesgo*, en el rango numérico de 0 a 9 (explicado de manera detallada en el **Anexo B.2** "*Tabla N° 1. Valores según el nivel de criticidad*").

Las dimensiones de valoración son otro punto fundamental que se debe poner en consideración, es saber cuáles son las consecuencias que traería si se materializaría una amenaza.

De un activo es interesante saber que hay diferentes dimensiones:

- Confidencialidad: ¿Cómo sería si las personas no autorizadas accedan a la información?
- Disponibilidad: ¿Qué hacer si no pueden acceder al sistema informático producido por un sabotaje?
- Integridad: ¿Qué hacer si la red de comunicaciones ha sido interceptada, para fines no éticos?

Las dimensiones antes nombradas permitirán valorar a cada uno de los activos de una manera simple guiado por la siguiente tabla llamada "criterios de valorización de activos" (**Anexo B.2** "*Tabla N°2: criterios de valorización de activos*") donde se muestra cuáles son los dimensiones que se usaron para la correcta valorización de los activos.

d) Identificar Amenazas

Según la ISO/IEC 27001 como parte del ciclo de vida de un SGSI, es necesario la identificación de las amenazas y vulnerabilidades a los que se encuentren

expuestos los activos de información e identificar las debilidades en la seguridad de la información que puedan amenazar a los activos de información de la DREP.

Los autores Fernández, y otros (2003) sostienen que una *amenaza* es un perjuicio potencial provocado por un incidente deseado o no deseado, hacia todos los activos de una organización. Si se llegara a ejecutar la amenaza puede poner en peligro la confidencialidad, integridad y disponibilidad de un activo.

Con este concepto nos da entender que es importante determinar las amenazas de todos los activos que cuentan con un nivel alto de criticidad, ya que pone en peligro la seguridad de la organización.

De acuerdo con el Anexo C (Estándar Internacional ISO/IEC27005, 2008) las categorías de amenazas o fuentes de amenazas se pueden clasificar en:

- A-daño físico
- B-Eventos Naturales.
- C-Perdida de servicios esenciales
- D-Perturbación por radiación.
- E-Compromiso de la información.
- F-Fallas técnicas
- G-Acciones no autorizadas
- H-Compromiso de las funciones
- I-Errores humanos
- J-Fallas en la gestión y la operación del servicio.

Como también Fernández, y otros (2003) definen que una *Vulnerabilidad* es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño".

Es por eso que las *vulnerabilidades* no pueden dañar a los activos por si solos, ya que son características propias de estos; sin embargo, deben ser

identificadas debido a que son fuentes potenciales de riesgos en caso logren ser explotadas por alguna *amenaza*.

Por último, los riesgos se definieron como aquella *probabilidad* de que una amenaza explote alguna vulnerabilidad haciéndole perder alguna propiedad relacionada a la seguridad de la información (confidencialidad, disponibilidad, integridad) de ahí la necesidad de identificar las amenazas y vulnerabilidades previamente. Para ello se realizó una previa visita a las áreas donde se llevan a cabo el proceso de contratación de personal docente y se utilizó una lista de ejemplos de vulnerabilidades y amenazas proporcionadas por el anexo D de la ISO/IEC 27005.

e) Determinar la probabilidad e impacto

Para la Determinación de la Probabilidad e Impacto se debe llevar en conjunto con los propietarios de los activos de información, deben contestar las siguientes preguntas para determinar la probabilidad de ocurrencia de una amenaza:

¿Ya ha sucedido antes?, ¿pasa muy seguido? y ¿podría suceder?

De igual forma, se debe determinar cuál es el impacto que tendría a la materialización de la amenaza considerando la vulnerabilidad y los controles existentes.

El ***nivel de los riesgos*** se obtendrá de la multiplicación de la probabilidad y el impacto previamente definido por los propietarios del proceso lo cual permitirá ubicar al riesgo, se muestra en el **Anexo B.4** "*Tabla N°5. Matriz de Calor*"

A continuación se describen los niveles de riesgo:

Riesgo Relevante – Moderados - Bajo: riesgos inferiores, deben ser tratados con los procedimientos de rutina ya definidos en la organización. Es hasta este punto en el cual se define el apetito del riesgo de la DRE Piura, es decir, aquellos riesgos que no se encuentren en esta zona deberán ser tratados para minimizar su valor.

Riesgo Alto: Riesgos que deben ser tratados con procedimientos especiales con la ayuda de la implementación de algunos controles de seguridad, la alta dirección debe ser consciente de la existencia y tratamiento de estos riesgos.

Riesgo Crítico: Riesgos que deben ser tratados de manera inmediata y con alta prioridad debido a lo que podría suceder si se materializa el riesgo, la alta dirección debe ser consciente de la existencia y tratamiento de estos riesgos.

Luego de definir los niveles de riesgos respecto a las vulnerabilidades de cada activo y las amenazas que puedan afectar su integridad, confidencialidad o disponibilidad; se definió el tratamiento de los riesgos cuyo nivel sea “Crítico” o “Alto” es recurrir a la implementación de ciertos controles para reducir la probabilidad que dichos riesgos identificados se materialicen. Finalmente, no se requerirá de tratamiento para los niveles de riesgos de “Relevante”, “Moderado” y “Bajo” ya que se considera que la DREP puede convivir con dichos riesgos.

f) Identificar Controles

Los controles son medios para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, practicas o estructuras organizacionales; para reducir, retener, evitar o transferir los riesgos y se debería definir un plan para tratamiento del riesgo.

La (NTP ISO/IEC 27001:2014) muestra en el Anexo A los Objetivos control y controles que se derivan y alinean directamente con los que figura en NTP-ISO/IEC 17799-2007, en la tabla A.1-Objetivos control y controles donde la organización puede considerar que son necesarios objetivos control y controles adicionales, ya que estos ofrecen asesoría de implementación y pautas sobre las mejores prácticas en apoyo a los controles.

1.4 Formulación del problema

1.4.1 Pregunta General

- ¿cómo el análisis de riesgos evalúa los activos de información del proceso de Contratación de Personal Docente en la DREP basado en las directrices del ISO/IEC 27005?

1.4.2 Preguntas Específicas

- ¿Cómo se lleva a cabo el proceso de contratación de personal docente en la DREP?

- ¿Qué activos de información se identifican en el proceso de Contratación de Personal Docente en la DREP?
- ¿Qué amenazas y vulnerabilidades se identifican de los activos de información del proceso de Contratación de Personal Docente en la DREP?
- ¿Qué controles se proponen ante las amenazas identificadas de los activos de información del proceso de Contratación de Personal Docente en la DREP?

1.5 Justificación del estudio

Con la presente investigación análisis de riesgos de los activos de información del proceso de contratación de personal docente, se pretende evaluar la situación actual en la que se encuentran expuestos los activos de información del proceso de contratación de Personal Docente en la DREP, basado en las directrices del ISO/IEC 27005.

El trabajo de investigación se justifica de manera metodológica debido a que es factible llevarse a cabo, debido a que se basa en las directrices de la ISO/IEC 27005, tratando de llevar a cabo un análisis más detallado sobre el manejo de sus activos, a fin de evaluar los posibles riesgos para poder tomar medidas de acción sobre ellos, permitiendo obtener los niveles de riesgos a los que están expuestos cada activo en el proceso de contratación de personal docente en la DREP.

Al llevarse a cabo este proyecto de investigación, será de mucha ayuda al sector estatal, en especial la DREP, ya que no consideran realizar un análisis de riesgos a sus activos; es por eso que se toma la iniciativa de realizar un análisis de riesgos, basándose en las directrices del ISO/IEC 27005.

Con la elaboración de este proyecto se enfoca en aportar información útil tanto a la alta Dirección de la DREP como para los demás funcionarios, donde se pueda conocer de forma precisa cual será el ambiente más favorable, para tener una mejor seguridad de la información, para luego proponer controles seleccionando procedimientos de protección proporcionales a los riesgos establecidos y el valor de los elementos a proteger.

1.6 Hipótesis

El análisis de riesgos permitirá evaluar la situación actual en la que se encuentran expuestos los activos de información en el proceso de contratación de Personal Docente en la DREP, basado en las directrices del ISO/IEC 27005.

1.7 Objetivos

1.7.1 Objetivo General

- Analizar los riesgos evaluando los activos de información del proceso de Contratación de Personal Docente en la Dirección Regional de Educación de Piura, basado en las directrices del ISO/IEC 27005.

1.7.2 Objetivos Específicos

- Describir el proceso de Contratación de Personal Docente en la DREP.
- Identificar los activos de información del proceso de Contratación de Personal Docente en la DREP.
- Identificar vulnerabilidades y amenazas de los activos de información del proceso de Contratación de Personal Docente en la DREP.
- Proponer controles ante las amenazas identificadas de los activos de información del proceso de Contratación de Personal Docente en la DREP.

II. MÉTODO

2.1 Diseño de Investigación

La investigación es de tipo descriptiva, ya que incluye detalles del proceso de Contratación de Personal Docente en la DREP, para el Análisis de Riesgos de los Activos de información, simbólicamente se representa:

Donde G son: los activos de información del proceso “Contratación de Personal Docente” en la Dirección Regional de Educación”.

Donde O es: Análisis de riesgos.

2.2 Operacionalización de varible

Variable: Análisis de Riesgos de los Activos de Información.

VARIABLE	DEFINICION CONCEPTUAL	DEFINICION OPERACIONAL	DIMENSIONES	INDICADORES
Análisis de Riesgo de los activos de información	*"El objetivo del análisis de riesgos es identificar riesgos basados en la identificación de los activos, de sus amenazas y vulnerabilidades"* (**Alexander, 2007**)	El análisis de riesgos que se realiza a los activos de información del proceso de contratación de Personal Docente, se identifican los activos que tengan un nivel de criticidad ALTA para identificar sus amenazas y vulnerabilidades con el cual se mide el nivel de probabilidad e impacto de estos, que da como resultado el nivel de riesgo y así proponer controles preventivos y correctivos.	**Activos**	Porcentaje de Activos por tipología
				Nivel de criticidad
			Amenazas y Vulnerabilidades	Porcentaje de Amenazas
				Nivel Probabilidad de afectación
				Nivel Impacto en la organización.
				Nivel de riesgo
			Controles	controles propuestos

Tabla Nº 01: Cuadro de Operacionalización de Variable.

Elaboración propia.

2.3 Población y Muestra

La unidad de análisis para la presente investigación son los activos de información identificados en la contratación de personal docente de la Dirección Regional de Educación de Piura.

UNIDAD DE ANÁLISIS	
Activos identificados en el proceso de contratación de personal Docente.	**62**
Muestra	**21**

Tabla Nº 02: Unidad de Análisis.

Elaboración propia.

Para la unidad de análisis se tendrán en cuenta todos los activos que intervienen en el proceso de Contratación personal docente en la Dirección Regional de Educación. Pero solo a los activos que tengan un nivel de criticidad “ALTA” se tomaron en cuenta como muestra para la evaluación de riesgos para así proponer controles para mitigar los riesgos.

2.4 Técnicas e instrumentos de recolección de datos, validez y confiabilidad.

Para el análisis de riesgos de los activos de información, los primeros pasos que se realizaron fue la identificación de los activos de información según su tipología mediante una guía de observación; así como identificar el tipo de amenazas según su origen, para luego identificar el nivel de riesgo según la probabilidad que una amenaza explote una vulnerabilidad de un acto activo.

Para identificar los activos de información, las amenazas y vulnerabilidades de manera general para el análisis de riesgo en el proceso de Contratación de personal Docente.

El cuestionario sirvió para obtener opiniones de los propietarios de cada uno activos de información con respecto a la valorización donde se tuvo en cuenta

las dimensiones de la seguridad de la información; así como que incidentes y tipo de amenazas que ocurren en el proceso de contratación de Personal Docente.

INDICADORES	INSTRUMENTO
Porcentaje de Activos por tipología	Guía de observación N° 01
Nivel de criticidad	Guía de observación N° 02
Porcentaje de Amenazas por Tipología	Guía de observación N° 03
Nivel Probabilidad de afectación	Cuestionario N° 01
Nivel Impacto en la organización	Cuestionario N° 02
Nivel de riesgo	Matriz de calor
Controles	Guía de observación N° 3

Tabla Nº 03: Técnicas e Instrumentos de Recolección de Datos.
Elaboración propia.

2.5 Métodos de análisis de datos

Una vez obtenido los datos e información de los diferentes entes involucrados y corroborando con la visita a las distintas instalaciones de la DREP, se procedió a la revisión, análisis e interpretación de los mismos. Para ello se aplicaron métricas cualitativas.

Para el análisis de los Datos se estudian los resultados organizados en tablas de Excel. En este caso para identificar y valorar los activos, el porcentaje de los

activos con un nivel de criticidad “ALTA” en el proceso de contratación de personal Docente según los criterios de la seguridad de la información, así como como el porcentaje de amenazas y vulnerabilidades por cada activo para el análisis y evaluación del riesgo.

2.6 Aspectos éticos

La información obtenida durante el estudio en la Dirección Regional de Educación de Piura, será usada únicamente con fines académicos, sin fines de lucro y en beneficio único de la organización. Esta investigación cuenta con la autorización y el completo consentimiento de la entidad en cuestión a través de un documento que hace constancia de ello, así mismo el investigador actúa bajo el ámbito legal que enmarca la Legislatura Peruana.

III. RESULTADOS

El objetivo principal de la investigación es analizar los riesgos evaluando los activos de información del proceso de Contratación de Personal Docente en la DREP. Para realizar el análisis de riesgos detallando el manejo de sus activos y a fin de evaluar los posibles riesgos, se tomaron en acción las siguientes etapas.

Como primera etapa el proceso de contratación de personal docente se distinguió como alcance esta investigación.

Siguiendo como segunda etapa del análisis de riesgo, se identifican los activos de información por tipología que intervienen en el proceso de contratación de Personal Docente en la DREP, se encontró un 33% de tipo “Datos” en su gran mayoría, ya que la DREP desde el área de Trámite documentario se maneja información curricular del Docente y con un formulario único de trámite, hasta el término de la contratación se obtiene como información y constancia, con el documento del Proyecto de Resolución Directoral de Piura, con el propósito de formalizar el vínculo contractual del servidor civil según los términos del contrato y las disposiciones vigentes.

Como también intervienen datos sobre los cargos que se emiten a cada área encargada según sus funciones.

Luego se obtuvo un 29% de tipo “Personal” ya que es parte fundamental para la organización puesto que maneja la información y maneja cada uno de los procesos que tiene la institución, y también recaen las responsabilidades según sus funciones. Con un 14% se obtuvo de tipo “Aplicación”, aquí se encuentran las licencias de los sistemas operativos que tienen los computadores así como los servidores para conectarse con la base de datos de los sistemas de información NEXUS y STD, los cuales se manejan para realizar el registro de los expedientes en el caso del sistema de Tramite documentario y para la verificación de la existencia de plazas codificada por NEXUS (Sistema para la Administración y Control de Plazas docentes, administrativos del sector educación). Otro activo importante es la página web de la DREP, ya que es un medio donde se emiten comunicados y la base de datos del sistema NEXUS de la DREP. El tipo de activo “Equipamiento Auxiliar” obtuvo un 10% ya que aquí se encuentran los archivadores para los documentos, es donde se tienen

clasificados y foliados los documentos de los docentes de todas las áreas que intervienen en este proceso como son Área de Gestión Institucional, asesoría legal, Área de personal como tramite documentario por otro lado está el sistema de alimentación eléctrica o llamado UPS.

Como siguiente tipo activo identificado es de “Tecnología” con un 8%, encontramos los computadores de escritorio donde solo las áreas de trámite documentario y personal la utilizan para registrar y verificar datos sobre los postulantes (docentes) para las plazas en las que se ha concursado, también encontramos cables de Ethernet para conectarse a la red así es como se identificó con un 4% activos de tipo “Red”, donde encontramos los periféricos que se utilizan para comunicación de redes como son los Switch, Router y HUB. Por último encontramos los activos de tipo “Instalación” con un 3% es aquí donde resguardan los equipos de cómputo y los servidores que las oficinas y en especial la oficina del “centro de cómputo” de la DREP donde se protegen los equipos de red protegido en el “cuarto de frío”, así como también las vitrinas informativas se utilizan para emitir comunicados y relación de los docentes con sus respectivas proyectos de Resolución Directoral.

Como tercera etapa se identifica el nivel de criticidad considerando las dimensiones de la seguridad de la información que son la integridad, disponibilidad y confidencialidad, estas se tomaron como criterios para dar como resultado el nivel de criticidad con las escalas cualitativas “ALTA”, “MEDIA” y “BAJA”; teniendo como resultado que todos los activos de información implicados en el proceso de contratación de personal docente, solo un 2% obtuvo un nivel de criticidad “BAJA”, ya que el valor que obtuvo fueron bajos en los criterios de integridad y disponibilidad tomando en cuenta ciertas descripciones como fue el caso de las vitrinas informativas. El nivel de criticidad “MEDIA” fue de un 67% que se dio del total de los activos, ya que se tomaron en cuenta el valor que se le da a los criterios de integridad, disponibilidad y confidencialidad y por último el nivel de criticidad “ALTA” fue de un 31%, donde encontramos a los activos de tipo tecnológico, aplicación, datos, red e instalación, así lo dieron a evidenciar los propietarios de cada activo, así como el encargado del centro de cómputo, que se rige a dar mantenimiento y soporte de toda los activos tecnológicos que tienen las demás áreas y también maneja los equipos de redes de la DREP.

En la cuarta etapa se identificó las amenazas; para esta se clasificaron las amenazas por categorías a los activos que obtuvieron un nivel de criticidad "*ALTA*", ya que estos activos se les debe tener más consideración porque se ha visto que hay notorias vulnerabilidades, es por ello que se realizó entrevistas a los dueños de los activos con la intención de identificar las vulnerabilidades.

Las vulnerabilidades con mayor referencia por los entrevistados o identificadas durante las visitas a las áreas.

Los pocos o nulos controles de acceso a los activos tuvieron un 30%, otra vulnerabilidad común es la sensibilidad a la humedad, polvo y calor con un 29%, la falta de mecanismos de backup para la base de datos como los libros de cargos de las diferentes áreas fue de un 26%, otra vulnerabilidad referenciada es la gestión inadecuada de la red con7%, lo que no debe tener esta vulnerabilidad un centro de cómputo, ya que es parte vital para que el proceso de contratación de personal docente, para que no se saturen los sistemas de información, otras vulnerabilidades que se identificaron fueron falta de una adecuada gestión de reemplazo o mantenimiento y la falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería con 4% respectivamente. Siendo estas vulnerabilidades las más comunes que se encontraron en el proceso de contratación de personal docente.

Luego se identificaron las amenazas por categorías siendo l a categoría más alto porcentaje y que más debe preocupar a la DREP es el correspondiente al "compromiso de la información", ya que abarca amenazas como robo y manipulación del activo, pérdida de documentos, manipulación entre otros.

La categoría Daño físico concentra amenazas como contaminación, polvo y corrosión, temperatura o humedad externa, se ubica en el segundo lugar debido a que las condiciones físicas del centro de cómputo y demás áreas.

El centro de cómputo no cuenta con proyectos confiables para realizar un apropiado funcionamiento y operación de los recursos críticos de la organización.

Las fallas técnicas se deben particularmente a que la DREP por error al uso del software, otras amenazadas por la falta de mantenimiento de cables ósea hay caídas de red y es parte fundamental la disponibilidad que debe tener estos activos de tipo de red en general un centro de cómputo donde hace falta un sistema de cableado ya que actualmente el sistema de cableado en la DREP

tiene más de 15 años de antigüedad aunque lo recomendable son solo 10 años.

Las principales amenazas identificadas fueron; robo o manipulación de activos con un 43%, donde existen errores humanos, ya que la documentación de la DREP como en este caso los libros cargos de las diferentes áreas que intervienen en el proceso de contratación de personal docente.

La contaminación, polvo y corrosión se obtuvo un 20% por parte de los activos de tipo tecnológicos como los computadores y servidores de centro de cómputo de la DREP. Mientras que el abuso de derechos obtuvo un 14% por falta de registros de auditorías.

En la quinta etapa se determinó la probabilidad e impacto, para obtener como resultado el nivel del riesgo.

Para cada una de las amenazas identificadas explotada por una vulnerabilidad se investigó la probabilidad de ocurrencia y el impacto estimado en la organización. Con ayuda de los cuestionarios y regidos de tablas con su puntaje respectivo, para identificar el nivel de Probabilidad como también el nivel de impacto hacia la DREP.

Para dar como resultado el nivel de riesgo que se obtendrá de la multiplicación de la probabilidad y el impacto previamente definido por los propietarios del proceso, teniendo de referencia la matriz de calor. Como resultado se obtuvo un nivel “Critico” de un 25% del total de amenazas de todos activos siendo el nivel en los que deben ser tratados de manera inmediata y con alta prioridad debido a lo que podría suceder si se materializa el riesgo, los activos de tipo “Red” fueron los que obtuvieron este nivel. El nivel “alto” obtuvo un 50% donde se encontró a los activos de tipo dato, en este nivel deben ser tratados con procedimientos especiales con la ayuda de la implementación de algunos controles de seguridad. El nivel “relevante” alcanzo un 25%, se encontraron riesgos inferiores, que deben ser tratados con los procedimientos de rutina ya definidos en la organización, para minimizar su valor

IV. DISCUSIÓN

En este capítulo se efectuó el análisis y su respectiva interpretación de los resultados obtenidos en el capítulo anterior, de acuerdo al variable análisis de riesgos de los activos de información, la misma que sirvió para efectuar cálculos estadísticos e indicadores.

Para el desarrollo de la investigación como primera etapa se definió el alcance, se tomó al proceso de contratación de personal docente; así lo considera la ISO/IEC 27005 en trabajar sobre procesos ya que facilita el entendimiento sobre el funcionamiento de la organización, así como la investigación de Aguirre (2014) considero los procesos “core” de la empresa Serpost como por ejemplo recepción de encomiendas, como también la investigación de Aliaga (2014) tomo los procesos más importantes de un instituto educativo como por ejemplo el proceso de admisión de un estudiante. Por lo tanto se comprueba que es importante definir el alcance porque nos da conocer el manejo de información que tiene la organización.

Con respecto al indicador N° 1: Porcentaje de activos por tipología, se identificaron los activos según los siete tipos definidos por la ISO/IEC 27005. En este caso los activos más importantes que maneja la DREP son de tipo dato, pero este depende de otros activos base como son de tipo tecnológico, aplicación y el personal; es por eso que con la realización del análisis de riesgos se realizó un inventario de cada activo según su tipo, quien es el responsable, y una breve descripción de la actividad que realiza en el proceso de contratación para que así la DREP tenga una constancia de la importancia de cada activo.

En cuanto al indicador N° 2: el nivel de criticidad se tomó en cuenta las dimensiones de la seguridad de la información como son la disponibilidad, la confidencialidad e integridad, observando que los activos que obtuvieron criticidad “alta” fueron los de tipo dato, tecnológico y aplicación. Por lo que al demostrar estos resultados la DREP debe tomar medidas de seguridad para regular como también para que haga un plan de inversión ya que son activos

base para el manejo de información como son el red de cableado y sistemas operativos.

Del indicador N° 3: porcentaje de amenazas por categoría, se puede apreciar que no tenían identificadas mediante documento el registro de amenazas que pueden afectar a cada uno de los activos, con ayuda del análisis de riesgo, se elaboró un listado de amenazas y vulnerabilidades identificadas que están plasmadas dentro del documento llamado plan de Análisis de Riesgos. Demostrando que con un 43% son más vulnerables a la amenaza de robo o manipulación del activo.

Del indicador N° 4: Nivel de probabilidad, se estableció una tabla cuantitativa indicando el nivel desde Muy alto hasta muy bajo, para medir el nivel en que pueden ser explotadas las vulnerabilidades existentes se tuvo en cuenta los siguientes factores: según los motivos de las fuentes de la amenaza y su dimensión (la capacidad para hacer daño), la naturaleza de la vulnerabilidad así como la existencia y efectividad de controles existentes.

Del indicador N° 5: Nivel de impacto, se estableció una tabla cuantitativa indicando el nivel desde muy alto hasta muy bajo, teniendo en cuenta que el impacto adverso de un evento de seguridad, también es necesario tener en cuenta que costo aproximado tendría cada ocurrencia así como una mala la imagen de la Dirección Regional de Educación de Piura ya que esta es una organización estatal del sector educativo.

En el indicador N°6: Nivel de riesgo, para determinar el nivel de riesgo se multiplican el nivel de la probabilidad por el nivel del impacto, como se muestra en la matriz de calor. La escala de riesgo, con niveles desde “muy bajo” hasta “crítico”, representando el grado o el nivel a que se encuentra expuesto el activo de información evaluado, en la DREP se obtuvo un 25% de nivel “crítico” de los activos evaluados por lo que se le ha propuesto que controles tiene que poner en marcha para que el nivel de riesgo se disminuye, más que todo porque pone enfilo activos de tipo dato, como son los libros de control y resoluciones directorales que son parte fundamental para este proceso de contratación.

Por los resultados obtenidos se logra demostrar que la hipótesis del análisis de riesgos basado en las directrices del ISO/IEC 27005 permitirá evaluar la

situación actual en la que se encuentran expuestos los activos de información del proceso de contratación de personal de la DREP es considerada, teniendo en cuenta que se encontró un 34% de activos con alta criticidad, por lo que aportó a la DREP a obtener información sobre los riesgos, amenazas, y protecciones que deben considerar para evitar y tomar medidas de prevenciones oportunas y adecuadas.

V. CONCLUSIONES

Luego de haber realizado la investigación en DREP se puede concluir lo siguiente:

- El proceso de contratación de personal docente de la DREP se estableció como alcance de la investigación, se reconocieron las áreas involucradas, realizando entrevistas con los dueños de cada área para recolectar información necesaria; de como realizan su trabajo en el área, a fin de asociar los activos identificados dentro del proceso, con el propósito de facilitar la labor de análisis y evaluación de riesgos se modelo el proceso de contratación de personal docente de la DREP utilizando la notación BPMN 2.0.

- Al identificar los activos de información que intervienen en el proceso de Contratación de Personal Docente en la DREP, se registró la tipología, el responsable de cada activo, el flujo que tiene en el proceso, así como la descripción de ellos, con el propósito de obtener el inventario correspondiente para describir de manera real cuál es su función.

- Al identificar las vulnerabilidades y amenazas de todos los activos con alta criticidad, los de tipo red obtuvieron un “ALTO” nivel de riesgo debido a que no hay una planificación del sistema de cableado, aparte de la antigüedad de la red de más de 15 años, por lo que genera caídas de red y por consecuencia demoras en los procesos administrativos; así como también se encontró niveles de riesgo “CRITICOS” por los pocos o nulos controles de acceso a los activos tecnológicos y activos de tipo dato.

- Se ha calificado controles que ayudarán a mitigar o reducir los riesgos identificados, de ser aprobada la propuesta, un 70% implicaría buenos resultados en la efectividad del proceso de contratación de personal Docente de la DREP, sobre todo porque se proponen procedimientos a seguir por cada control, esto es el producto de los anteriores etapas

realizadas en el análisis de riesgo, caso contrario se tomarían acciones a largo plazo.

VI. RECOMENDACIONES

- En esta investigación solo se tomó en cuenta el proceso de contratación de personal docente, se recomienda a los altos directivos, tomar en cuenta los demás procesos que tiene la DREP ya que también intervienen otras áreas, para así evaluar que riesgos más se podrían encontrar, ya que por el tiempo en que se realizó la investigación no se amplifico en los demás procesos que intervienen.

- Se recomienda a los Altos directivos de la DREP, tener como prioridad la evaluación de riesgos de los activos de tipo tecnología, red, datos y personal, ya que no se tiene en cuenta las amenazas y vulnerabilidades que constantemente son afectadas por factores internos como externos.

- Se recomienda Implementar procedimientos para controlar los accesos a las instalaciones de la DREP.

- Se recomienda efectuar los procedimientos siguiendo las normas de seguridad para la planificación de un sistema de cableado, ya que la antigüedad de la red es de 20 años, por lo que genera caídas de red y por consecuencia demoras en los procesos administrativos.

VII. PROPUESTA

PLAN DE ANALISIS DE RIESGOS

El presente documento describe los pasos necesarios para identificar y analizar los riesgos a los que se encuentra expuesta la organización, así como las acciones a realizar para el tratamiento de los mismos, en concordancia con lo propuesto por la ISO/IEC 27005:2008 referente a la gestión de riesgos en la seguridad de la información.

7.1 Planificación

7.1.1. Determinación del objetivo y alcance.

Evaluar el proceso de contratación de personal docente a fin de conocer la situación actual en la que se encuentran expuestos los activos de información basada en las directrices del ISO/IEC 27005.

El análisis de riesgos de los activos de información del proceso de contratación de personal docente.

Proponer objetivos control, controles para mitigar riesgos que se han identificado.

7.1.2 Actividades a realizar.

- Entrega de documentación de la DREP.
- Realización de Cuestionarios a los propietarios de las diferentes áreas.
- Desarrollo de la evaluación de riesgos del proceso de contratación de personal docente.
- Registro de información en guías de observación.

7.1.3 Análisis del ambiente y del entorno.

El análisis se basa en la observación del organigrama proporcionado por la organización y el manual de procedimientos; con ello se logra determinar que está bien organizada, siendo las áreas de tramite documentario, área de personal, área de gestión institucional, Dirección de Administración, Dirección de Asesoría Jurídica y la propia Dirección, no obstante aunque no se presente como una área, el centro de cómputo realmente es parte importante de las demás áreas administrativas por lo que también se tomó en cuenta para la investigación.

7.1.4 Determinación de los recursos Humanos.

- **Humanos.**
  - ✓ Investigadora: Katia Chunga Ramírez.
  - ✓ Asesor: Mg. Quito Rodríguez Carmen Zulema
- **Materiales:**

  - ✓ software Software: Microsoft Office Profesional Plus 2013.
    Adobe Reader DC.
    Windows 2010.
    Win Rar 4.0.

  - ✓ Hardware Laptop HP pavilion
    Multifuncional HP.

  - ✓ Servicios Internet
    Impresiones
    Anillados
    Fotocopias
    Transporte Urbano.

  - ✓ Varios Materiales

Memoria USB

Papel Bond A4

Folder Manila A4

7.2 Ejecución – Análisis de riesgos

7.2.1. Solicitudes de Manuales de procedimientos y Documentación.

Para la realización de esta actividad, se redactó un documento en el cual se solicitó la documentación básica, documentos e informacion con la que se debe contar toda la DREP, la cual fue dirigida al encargado de computo, ya que este funcionario fue al que se le designo para la ayuda de esta investigación.

Con esta solicitud se busca estudiar y describir el proceso de contratación de personal docente, así como demostrar si existe la existencia o no de documentación sobre buenas prácticas para la seguridad de la información.

Este proceso de contratación de personal docente se modelo siguiendo la notación BPMN 2.0 (Bussines Process Modeling Notation) la cual es una notación grafica estandarizada que permite observar de manera detallada todo el flujo de trabajo de dicho proceso.

Ver Anexo D2: formato de Solicitud de documentación.

7.2.2. Identificar Activos de información.

I. Cuestionario al encargado del centro de Computo.

En este punto se redactó y realizó una entrevista al encargado del centro de Cómputo; con la finalidad de verificar la existencia de documento de políticas de seguridad y datos referentes a los activos tecnológicos que intervienen en un proceso de contratación de personal docente.

VER: Anexo D: Cuestionario al encargado del centro de cómputo.

- Hallazgos potenciales

    - ✓ No existe políticas de seguridad de la información.
    - ✓ Se tiene documentado las funciones y objetivos de las áreas que intervienen en el proceso de contratación de personal docente.

II. Observación de las funciones del Área De Trámite Documentario, Área De Personal, Área De Gestión Institucional, Dirección De Administración, Dirección De Asesoría Jurídica Y A Dirección.

En este punto se realizó el llenado de la guía de observación N°1 donde se identifica cada uno de los activos; clasificándolo por su tipología, quien es el responsable y cuál es su función en el proceso de contratación de personal docente. Se realizaron entrevistas con los responsables de cada activo, así como también se guio por el manual de procedimientos administrativos

a) Identificación por tipología.
b) Asignación de responsables de cada activo, según su actividad.

. VER: Anexo B.1: Identificación de los activos

❖ Resultados de la Guía de observación

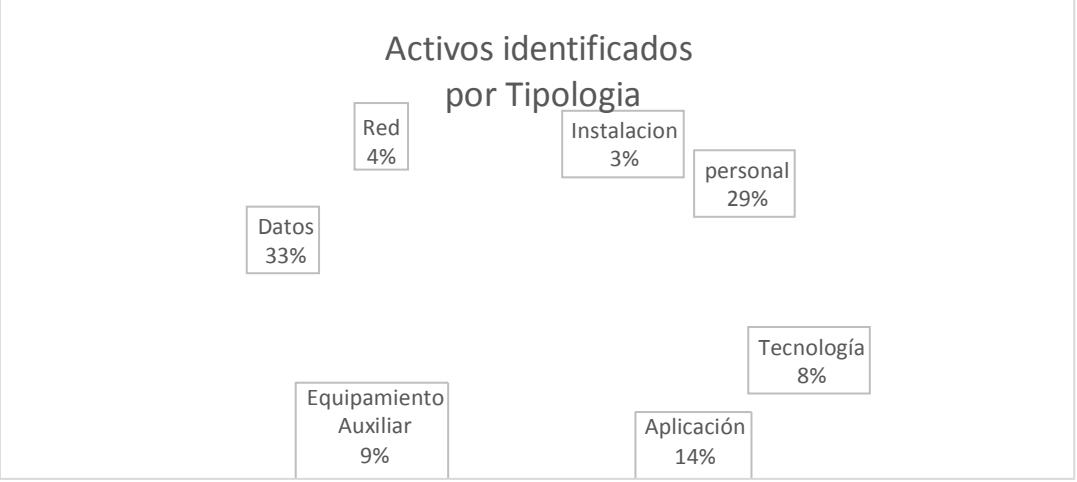


Figura Nº 02: Activos identificados por tipología.
Elaboración propia.

- Hallazgos
  - ✓ Las funciones de cada área del proceso de contratación de personal docente si están establecidas.
  - ✓ No se crean sistemas automatizados para la realización de las actividades (los sistemas son establecidos por el MINEDU desde la capital del Perú).
  - ✓ Las funciones del centro de cómputo no están establecidas como un área en específica.

III. Dimensiones de valorización para los activos de información identificados.

Para la dimensiones de valoración se aplicó una guía de observación para la valoración de los activos según el nivel de criticidad en la contratación de personal docente.

c) Establecer un puntaje sobre cada dimensión es necesario conocer la descripción de cada valor.

. VER: Anexo B.2: Valorización de los activos

- Resultados de la Guía de observación

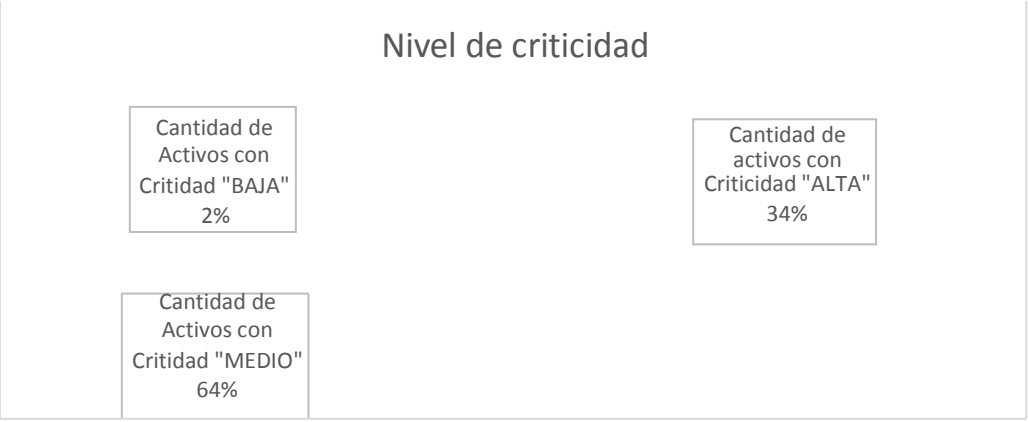


Figura Nº 03: Nivel de criticidad.

Elaboración propia.

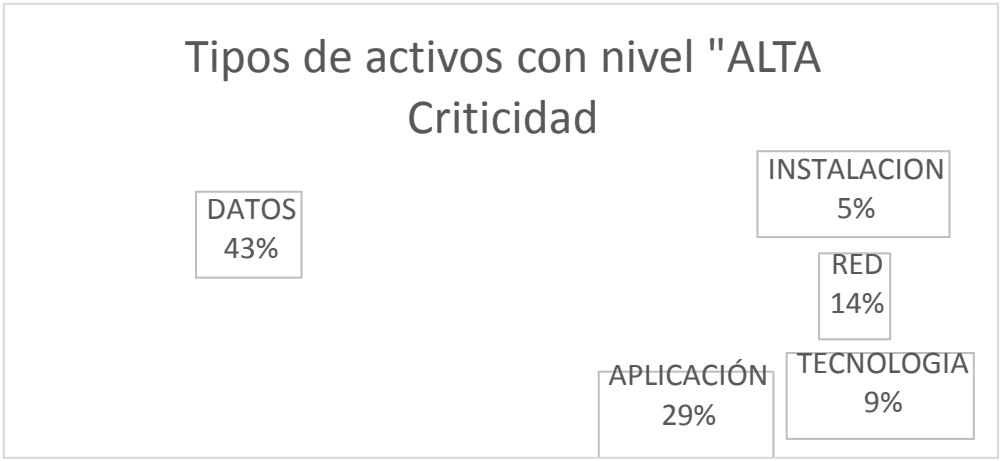


Figura Nº 04: tipos de datos que obtuvieron un nivel “Alta” de criticidad.

Elaboración propia.

- Hallazgos
    - ✓ Los niveles de criticidad que se identificaron son resultado de las entrevistas con los responsables de cada uno de los activos según la tabla de dimensiones de valorización de activos.
    - ✓ La mayor criticidad se halló en los activos de Tipo Dato.

IV. Identificación de amenazas y vulnerabilidades de los activos de información.

Para la identificación de las amenazas y vulnerabilidades se aplicó una guía observación teniendo en cuenta el "Anexo D de la ISO/IEC 27005:2008"

d) Establecer amenazas y vulnerabilidades.
e) Identificar las Amenazas más vulnerables.

VER: Anexo B.3: Matriz de riesgos

❖ Resultados de la Guía de observación.

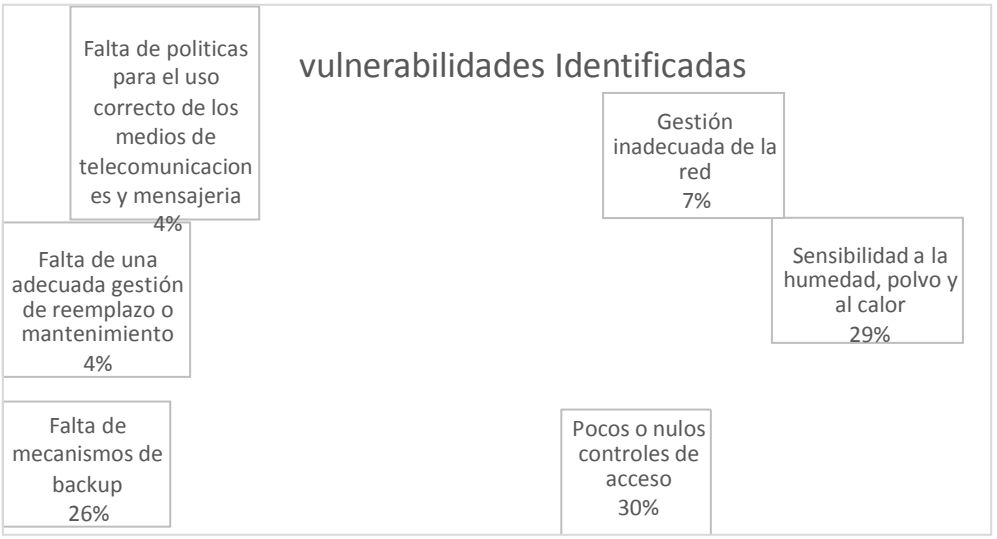


Figura Nº 05: Vulnerabilidades identificadas

Elaboración propia.

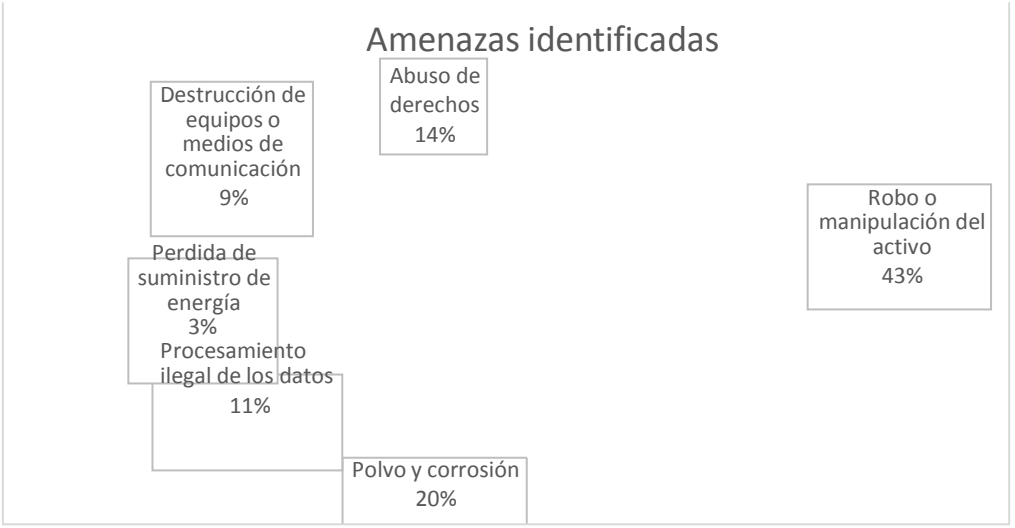


Figura Nº 06: Amenazas identificadas.

Elaboración propia.

- Hallazgos
  - ✓ Las amenazas identificadas con mayor porcentaje son tipo dato. Ya que son vulnerables a robo y manipulación.

V. Identificación y evaluación de riesgo

Para identificar el nivel de riesgo se utilizó una matriz de calor donde se calcula multiplicando el nivel de probabilidad de afectación por el nivel de impacto a la organización.

f) Determinar la probabilidad e impacto

Para determinar el nivel de probabilidad de afectación se realizó un cuestionario a los responsables de cada activo de informacion, teniendo en cuenta una tabla de lista de probabilidades. De igual forma, deben determinar cuál es el impacto que tendría a la materialización de la amenaza considerando la vulnerabilidad y los controles existentes. Para realizar la valorización se realizó un cuestionario teniendo en cuenta la tabla de lista de impactos.

g) Evaluación de nivel de riesgo

VER: Anexo B.6: Resultado de la matriz de riesgo.

- ❖ Resultados de la evaluación de riesgo

Figura Nº 06: Amenazas identificadas.
Elaboración propia.

- Hallazgos potenciales
  - ✓ Los activos de información de obtuvieron nivel crítico son de tipo datos, tecnológico, aplicación y red.

VI. Propuesta de controles

Para el tratamiento del riesgo se tomara el anexo de matriz de riesgo con los datos hallados, se deberá identificar que controles se tienen que implementar para minimizar los riesgos, ya sean técnicos o no.

Con la ayuda de la ISO/IEC 27001, se seleccionaron los controles adaptándolos a la organización.

h) Identificar controles según los riesgos

VER: Anexo B.7: Propuesta de controles

- Hallazgos potenciales
  - ✓ Se seleccionaron controles de acuerdo a los riesgos identificados para los activos de tipo datos, tecnológico, aplicación y red.

VIII. REFERENCIAS

AGUIRRE , DAVID. 2014. Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A. *Tesis para optar por el Título de Ingeniero Informático.* http://tesis.pucp.edu.pe/repositorio/handle/123456789/5677.

ALEXANDER, A. 2007. Diseño de un Sistema de Gestión de Seguridad de Información. Óptica ISO 27001:2005.

ALIAGA, LUIS. 2013. Diseño de un sistema de gestión de seguridad de información para un instituto educativo. *Tesis para optar por el Título de Ingeniero Informático. Perú.* http://tesis.pucp.edu.pe/repositorio/handle/123456789/4721.

AMPUERO, CARLOS. 2011. Diseño de un Sistema de Gestión de Seguridad de Información para una Compañia de seguros. *Tesis para optar por el Título de Ingeniero Informático.* http://tesis.pucp.edu.pe/repositorio/handle/123456789/933.

CUEVAS C. , RUDY . 2011. *Gerencia , gestión y liderazgo educativos.* [ed.] Jr. Dávalos Lissón. Primera . Lima : San Marcos E.I.R.L.Pág. 415. 978-612-302-482-6.

DIRECCION REGIONAL DE EDUCACION. 2007. Manual de Procedimientos Administrativos (MAPRO). Piura : s.n. 80 folios.

DONADO, SILER AMADOR Y FLECHAS, ANDRES. 2001. Seguridad Computacional. Primera edición Cauca. http://www.govannom.org/seguridad/seg_general/seg_com.pdf.

ESPINOZA, HANS. 2013. Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo. *Tesis para optar por el Título de Ingeniero Informático. Perú.* http://tesis.pucp.edu.pe/repositorio/handle/123456789/4957.

ESTÁNDAR INTERNACIONAL ISO/IEC 27001. iso27000.es. http://www.iso27000.es/sgsi.html.

ESTÁNDAR INTERNACIONAL ISO/IEC 27002:2007. Iso27000.es. http://www.iso27000.es/iso27002.html.

ESTÁNDAR INTERNACIONAL ISO/IEC27005. 2008. 27000 org. http://www.27000.org/iso-27005.htm.

FERNÁNDEZ, EDUARDO Y PIATTINI, MARIO. 2003. *Seguridad de las tecnologías de la Información: La construcción de la confianza para una sociedad conectada.* Madrid : Ediciones Aenor., 2003.

GARCIA, ALFONSO Y ALEGRE, MARIA DEL PILAR. 2011. *Seguridad Informática. Primera edición.* Madrid : Ediciones Paraninfo.

INTERNATIONAL STANDARD ISO/IEC 27000. 2014. *Publicada el 01/15/2014.* 2014.

MARTINEZ PONCE DE LEON, JESÚS G. 2007. *Introducción al análisis del riesgos.* Bogota : Limusa.

GÓMEZ RICARDO, ET AL. 2010. METODOLOGÍA Y GOBIERNO DE LA GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE LA INFORMACIÓN. n 31, s.l. : Revista de Ingeniería,p.109-118., 2010.

MONCAYO RACINES DIANA ELIZABETH. 2014. Modelo de evaluacion de riesgos de Tic´s de pequeñas y medianas empresas del sector Automotriz.

NTP ISO/IEC 27001:2014. INDECOPI. *Norma Técnica Peruana.* http://www.pecert.gob.pe/_publicaciones/2014/ISO-IEC-27001-2014.pdf.

NTP ISO/IEC 17799:2007. INDECOPI. *Publicada el 2007-08-22.* [Enhttp://www.ongei.gob.pe/normas/0/NORMA_0_RESOLUCI%C3%93N%20MINISTERIAL%20N%C2%BA%20246-2007-PCM.pdf.

OFICINA NACIONAL DE GOBIERNO ELECTRONICO E INFORMATICO (ONGEI). *Portal de Seguridad de Informacion.* http://www.ongei.gob.pe/entidad/ongei_tematicos.asp?cod_tema=4552.

PELTIER, THOMAS Y OTROS. 2005. *Information Security Fundamentals. USA.* s.l. : Auerbach Publications, 2005.

PÉREZ FERNÁNDEZ DE VELASCO, JOSÉ ANTONIO y DE VELASCO, JOSÉ ANTONIO PÉREZ.2007. *Gestión por procesos.* s.l. : ESIC Editorial.

MANUEL. 2011. PRINCIPIOS DE AUDITORÍA Y CONTROL DE SISTEMAS DE INFORMACIÓN**.** SEGUNDA. : Tupia Consultores y Auditores.

IX. ANEXOS

Anexo A: Instrumentos de Recolección de Datos

Anexo A.1: Constancia de haber realizado la investigación en la DREP

"AÑO DE LA CONSOLIDACIÓN DEL MAR DE GRAU"

Piura REGIÓN

GERENCIA REGIONAL DE DESARROLLO SOCIAL

DIRECCION REGIONAL DE EDUCACION DE PIURA

CONSTANCIA

DE INVESTIGACION

Por medio de la presente dejamos constancia que la ***Srta. Katia Chunga Ramirez,*** identificada con DNI N° 46219640, ha realizado una investigación titulada "Análisis de riesgos de los activos de información del proceso de contratación de personal docente de la Dirección Regional de Piura basado en las directrices del ISO/IEC 27005" en nuestra Área de Centro de Computo así como otras Áreas tales como Personal, Tramite documentario y Administración realizando las funciones de Asistente, desde Agosto del 2016 hasta el Noviembre del 2016.

Expedimos esta certificación a petición de la interesada para fines de ley que sea conveniente.

Piura, 14 de Octubre de 2016.

MINISTERIO DE EDUCACIÓN
DIRECCIÓN REGIONAL DE EDUCACIÓN
PIURA
Ing°. LUIS A. TORRES PRECIADO
ENCARGADO CENTRO COMPUTO

Luis A. Torres Preciado
Encargado del Centro de Cómputo

Anexo A.2: Guía de Observación N° 01

Análisis de Riesgos de los activos de Información del proceso de Contratación de Personal Docente en la Dirección Regional de Educación basado en las directrices de la ISO/IEC 27005.

GUÍA DE OBSERVACIÓN Nº 01:

Objetivo: Identificar los activos de información que son parte del proceso de contratación de personal docente basado en la metodología basado en la ISO/IEC 27005.

Datos generales:

Institución: Dirección Regional de Educación- PIURA.

Área: Trámite Documentario, Personal, Administración, Gestión Institucional, Asesoría Jurídica, Dirección General.

Responsable:

Fecha: ____/____/____

Tipos de Activos	Activo de información	Responsable	Actividad	Descripción del Activo
TECNOLOGIA				
APLICACION				
DATOS				
RED				
INSTALACION				

PERSONAL				
SERVICIOS				

NOTAS:

_____

_____

_____

Firma

Anexo A.3: Validez de guía de observación N° 01

Tipos de Activos	Activo de información	Responsable	Actividad	Descripción del Activo
TECNOLOGIA				
APLICACION				
DATOS				
RED				
INSTALACION				
PERSONAL				
SERVICIOS				

NOTAS:

MINISTERIO DE EDUCACION
DIRECCION REGIONAL DE EDUCACION
PIURA

Ing°. LUIS A. TORRES PRECIADO

Firma

Anexo A.4: Guía de Observación N° 02

Análisis de Riesgos de los activos de Información del proceso de Contratación de Personal Docente en la Dirección Regional de Educación basado en las directrices de la ISO/IEC 27005.

Guía de Observación N° 02

"Guía de observación para la valoración de activos según el nivel de criticidad en la contratación de Personal Docente en la DREP"

Objetivo: Dar una valoración a cada activo identificado previamente, en cada dimensión que corresponda. El puntaje o valoración será supervisado por la persona responsable del mismo.

Nota 1: Para establecer un puntaje sobre cada dimensión es necesario conocer la descripción de cada valor.

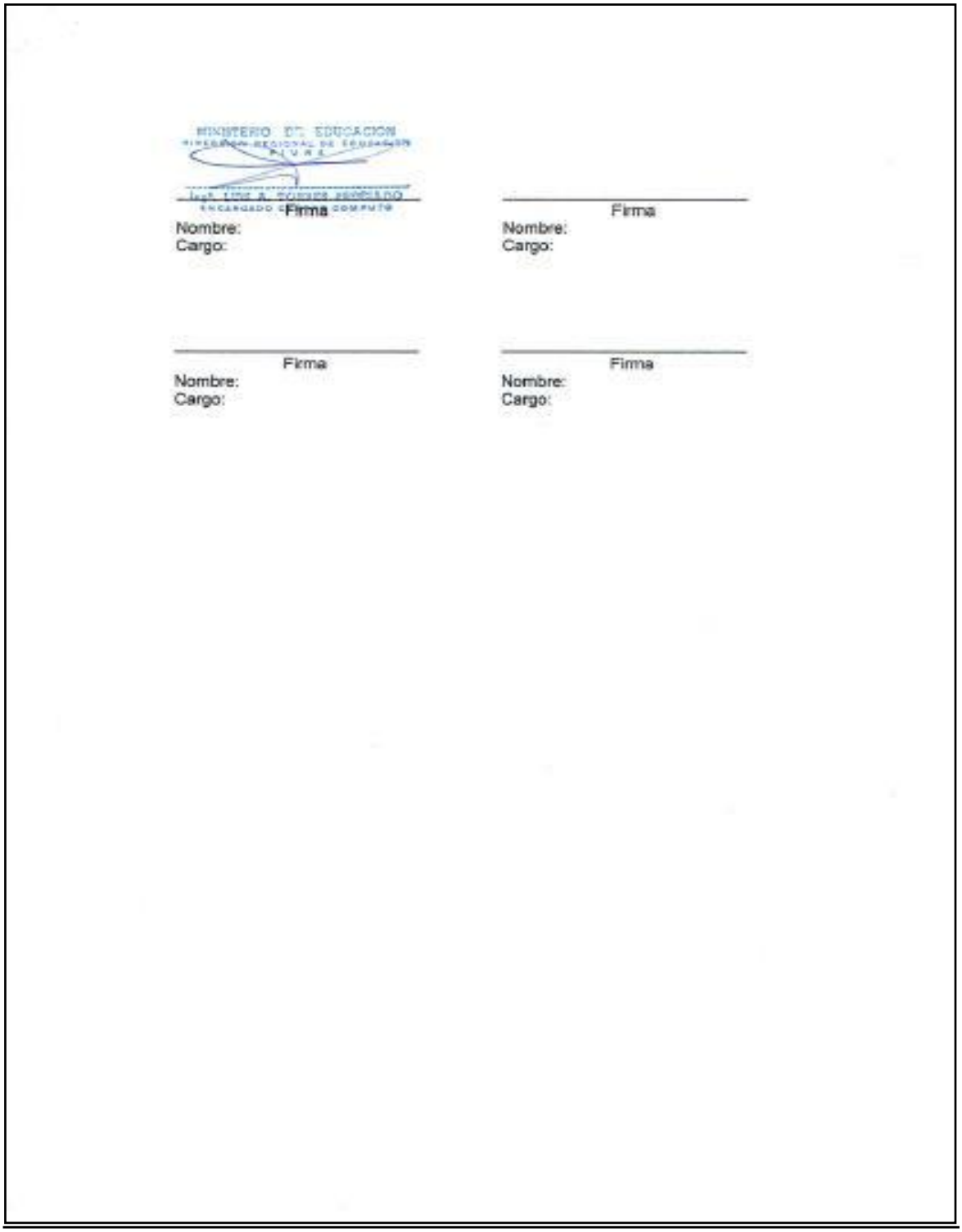
Fecha de inicio : ____/____/____
Fecha de término : ____/____/____

Dimensiones	Valor	Descripción
¿Qué valor le darías según la Integridad?	0	No aplica / No es relevante
	1	No es relevante los errores que tenga o la información faltante
	2	Tiene que estar correcto y completo al menos en un 50 %
	3	Tiene que estar correcto y completo en un 100%
¿Qué valor le darias según la Disponibilidad?	0	No aplica / No es relevante
	1	Debe estar disponible al menos el 10% del tiempo
	2	Debe estar disponible al menos el 50% del tiempo
	3	Debe estar disponible siempre
¿Qué valor le darías según la Confidencialidad?	0	No aplica / No es relevante
	1	Daños muy bajos, el incidente no transcendería del área afectada
	2	Seria relevantes, incidente implicaría a otras áreas
	3	Los daños serian catastróficos, la reputación y la imagen de la organización se verían comprometidas

Tipos de Activos	Nombre de Activo	Supervisado por	Dimensiones			T	Criticidad
			I	D	C		
Hardware	Computadora de Escritorio de Tramite Documentario y Personal						
	Laptop						
Tecnología	Cableado de Ethernet						
	Teléfono						
	Impresora						
	Fotocopiadora						
Aplicación	Licencia De Microsoft Windows XP						
	Licencia De Microsoft Office 2007						
	Red de la DREP						
	Firewall						
	sistema de información NEXUS y STD						
	Servicios de dominio						
	Servidor de archivos						
	Backup de archivo de usuarios						
	Servidores para el sistema Informático NEXUS (plazas codificadas) y STD						
	Página Web De La DREP						

Equipamiento Auxiliar	Archivadores para los documentos						
	Archivos de Asesoría Legal						
	Sello de transcripción						
	UPS (sistema de alimentación)						
	Sello de transcripción						
	Archivos de gestión Institucional						

Anexo A.5: Validez de guía de observación N° 02



Firma
Nombre:
Cargo:

Firma
Nombre:
Cargo:

Firma
Nombre:
Cargo:

Firma
Nombre:
Cargo:

Anexo A.6: Guía de Observación N° 03

Análisis de Riesgos de los activos de Información del proceso de Contratación de Personal Docente en la Dirección Regional de Educación basado en las directrices de la ISO/IEC 27005.

Guía de Observación N° 03

"Guía de observación para la identificación de amenazas y vulnerabilidades de los activos de información en el proceso de contratación de Personal Docente en la DREP"

Objetivo: identificar las amenazas y vulnerabilidades a cada activo, teniendo en cuenta la "lista de ejemplos de vulnerabilidades y amenazas" obtenido del "anexo D" de la ISO/IEC 27005:2008.

Nota 1: Para establecer el tipo de amenazas se tuvo en cuenta "lista de ejemplos de vulnerabilidades y amenazas" obtenido del "anexo D" de la ISO/IEC 27005:2008.

Fecha de inicio : ____/____/____
Fecha de término : ____/____/____

Tipo	Amenazas	Origen
Daño físico	Fuego	A, D, E
	Daño por agua	A, D, E
	Contaminación	A, D, E
	Accidente importante	A, D, E
	Destrucción del equipo o los medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado	A, D
	Pérdida de suministro de energía	A, D, E
	Falla en el equipo de telecomunicaciones	A, D
Perturbación debida a la radiación	Radiación electromagnética	A, D, E
	Radiación térmica	A, D, E
	Impulsos electromagnéticos	A, D, E
Compromiso de la información	Interceptación de señales de interferencia comprometedoras	D
	Espionaje remoto	D
	Escucha subrepticia	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A, D
	Datos provenientes de fuentes no confiables	A, D
	Manipulación con hardware	D
	Manipulación con software	A, D
	Detección de la posición	D
Fallas técnicas	Falla del equipo	A
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	A, D
	Corrupción de los datos	D

Figura N°7: Ejemplo de amenazas comunes
Fuente: Anexo C de la ISO 27005

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	• Piratería • Ingeniería social • Intrusión, accesos forzados al sistema • Acceso no autorizado al sistema
Criminal de la computación	Destrucción de información Divulgación ilegal de información Ganancia monetaria Alteración no autorizada de los datos	• Crimen por computador (por ejemplo, espionaje cibernético) • Acto fraudulento (por ejemplo, repetición, personificación, interceptación) • Soborno de la información • Suplantación de identidad • Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	• Bomba/terrorismo • Guerra* (warfare) de información • Ataques contra el sistema (por ejemplo, negación distribuida del servicio) • Penetración en el sistema • Manipulación del sistema
Espionaje industrial (Inteligencia, empresas, gobiernos extranjeros, otros intereses gubernamentales)	Ventaja competitiva Espionaje económico	• Ventaja de defensa • Ventaja Política • Explotación económica • Hurto de información • Intrusión en la privacidad personal • Ingeniería social • Penetración en el sistema • Acceso no autorizado al sistema (acceso a información clasificada, de propiedad y/o relacionada con la tecnología)
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales) por ejemplo, error en el ingreso de los datos,	• Asalto a un empleado • Chantaje • Observar información de propietario • Abuso del computador • Soborno de información • Ingreso de datos falsos o corruptos

Figura N°8: Fuente de Amenazas Humanas
Fuente: Anexo C de la ISO 27005

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información
	Falta de esquemas de reemplazo periódico.	Destrucción del equipo o los medios.
	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Falta de control de cambio con configuración eficiente	Error en el uso
	Susceptibilidad a las variaciones de tensión	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Copia no controlada	Hurto de medios o documentos
Software	Falta o insuficiencia de la prueba del software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Falta de pruebas de auditoría	Abuso de los derechos
	Distribución errada de los derechos de acceso	Abuso de los derechos
	Software de distribución amplia	Corrupción de datos
	Utilización de los programas de aplicación a los datos errados en términos de tiempo	Corrupción de datos
	Interfase de usuario complicada	Error en el uso
	Falta de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos

Figura N°9: Ejemplo de Vulnerabilidades
Fuente: Anexo D de la ISO 27005

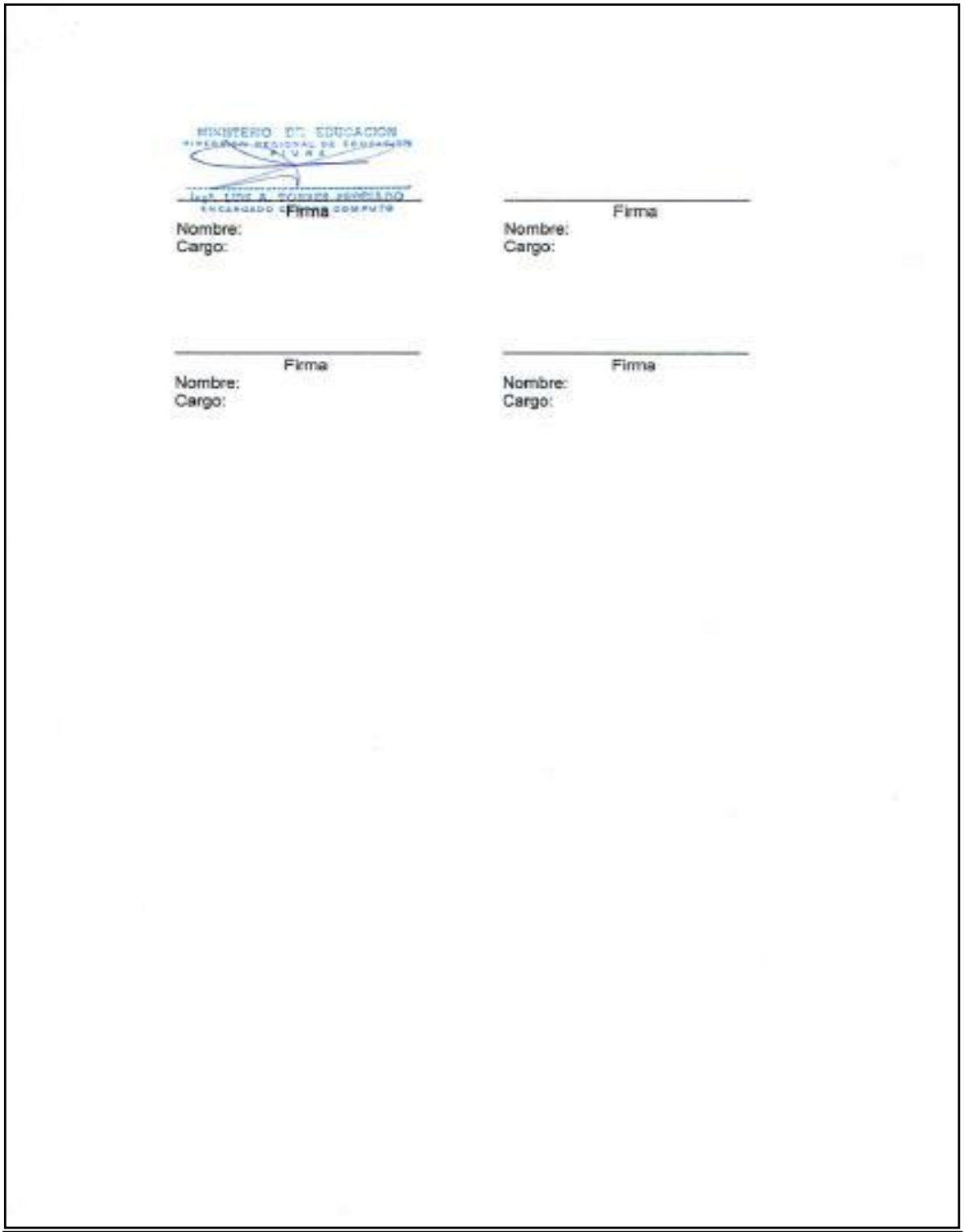
Software	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Falta de control eficaz del cambio	Mal funcionamiento del software
	Descarga y uso no controlados de software	Manipulación con software
	Falta de copias de respaldo	Manipulación con software
	Falta de protección física de las puertas y ventanas de la edificación	Hurto de medios o documentos
	Falla en la producción de informes de gestión	Uso no autorizado del equipo
Red	Falta de prueba del envío o la recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha subrepticia
	Tráfico sensible sin protección	Escucha subrepticia
	Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones
	Punto único de falla	Falla del equipo de telecomunicaciones
	Falta de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas autorizadas	Espionaje remoto
	Gestión inadecuada de la red (capacidad de recuperación del enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
	Ubicación en un área susceptible de inundación	Inundación
	Red energética inestable	Pérdida del suministro de energía
	Falta de protección física de las puertas y ventanas de la edificación	Hurto de equipo

Figura N°10: Ejemplo de Vulnerabilidades
Fuente: Anexo D de la ISO 27005

Activo	Vulnerabilidad	Amenaza
Computadora de Escritorio de Tramite Documentario y Personal	Falta de cierre de sesión al momento de salir de la estación de trabajo	Manipulación de información
	Sensibilidad a la humedad, polvo y al calor	Polvo, corrosión, congelamiento
	Susceptibilidad a variaciones en el voltaje	Perdida de suministro de energía
	Sensibilidad de golpes o caídas	Destrucción de equipos o medios de comunicación
	Falta de backups de información.	Robo de información o del mismo equipo
	Mala seguridad de contraseñas	Espionaje remoto

Tabla N°04: Ejemplo de Guía de observación N° 3
Elaboración Propia

Anexo A.7: Validez de guía de observación N° 03



Anexo A.8: Cuestionario N° 01

Análisis de Riesgos de los activos de Información del proceso de Contratación de Personal Docente en la Dirección Regional de Educación basado en las directrices de la ISO/IEC 27005.

CUESTIONARIO N° 01

Atención: Puntué sobre cada dimensión del activo que sea responsable. Cualquier consulta o duda no dude en preguntar al encuestador.

Requisito: Para establecer un puntaje sobre cada dimensión es necesario conocer la interpretación de cada escala de la probabilidad de afectación.

Probabilidad de Afectación	Interpretación
Muy Alta	Es casi seguro que la amenaza afectará la vulnerabilidad.
Alta	Es probable que la amenaza afecte la vulnerabilidad.
Media	Es posible que la amenaza afectara la vulnerabilidad.
Baja	Es improbable que la amenaza afectará la vulnerabilidad
Muy Baja	Es impensable que la amenaza afectará la vulnerabilidad

Fecha: Firma del encuestador

Responsable	Activo	¿Cuál es la probabilidad de que esta amenaza explote la vulnerabilidad?		Escala				
		Vulnerabilidad	Amenaza	Muy Alta	Alta	Media	Baja	Muy baja
Especialista administrativo	Computadora de escritorio	Falta de cierre de sesión al momento de salir de la estación de trabajo	Manipulación de la información					
	Cableado de Ethernet							
	Impresora							
	Fotocopiadora							
	Licencia De Microsoft Windows XP							
	Licencia De Microsoft Office 2007							
	Red de la DREP							
	Sistema de información NEXUS							

	Sistema de Tramite Documentario							
	Servidores							
	Página Web De La DREP							
	Archivadores para los documentos de todas las Áreas que intervienen en la contratación de personal Docente							
	Sello de transcripción							

Tabla N°05: Ejemplo de Cuestionario N° 1
Elaboración Propia

Anexo A.9: Validez de Cuestionario N° 01

Validez de contenido del cuestionario sobre la probabilidad de que una amenaza explote cierta vulnerabilidad de los activos de información en la contratación de Personal Docente en la DREP.

Estimado(a) Ingeniero/Maestro/Doctor:

Ing. Elmer Alfredo Chunga Zapata.

Siendo conocedor de su trayectoria académica y profesional, me he tomado la libertad de elegirlo como JUEZ EXPERTO para revisar el contenido del cuestionario que pretendo utilizar para determinarla probabilidad que hay en que cierta amenaza explote la vulnerabilidad.

A continuación presento una lista de afirmaciones (ítems) relacionadas a cada concepto teórico. Lo que se le solicita es marcar con una X el grado de pertenencia de cada ítem con su respectivo concepto, de acuerdo a su propia experiencia y visión profesional. No le pido que responda las preguntas de cada área, sino que indique si cada pregunta es apropiada o congruente con el concepto o variable que se pretende medir.

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido del presente cuestionario. De antemano agradezco su cooperación.

A. Información sobre el especialista

Sexo	: Varón (X) Mujer ( )
Edad	: 43 Años
Profesión o especialidad	: Ingeniero Informático
Años de experiencia laboral	: 13
No. ID. Colegio Profesional	: 90553

Anexo A.10: Cuestionario N° 02

Análisis de Riesgos de los activos de Información del proceso de Contratación de Personal Docente en la Dirección Regional de Educación basado en las directrices de la ISO/IEC 27005.

CUESTIONARIO N° 02

Atención: Puntué sobre cada dimensión del activo que sea responsable. Cualquier consulta o duda no dude en preguntar al encuestador.

Requisito: Para establecer un puntaje sobre cada dimensión es necesario conocer la interpretación de cada escala o impacto

Impacto en la Organización	Interpretación
Muy Alto	Pérdida o daño catastrófico a la reputación de la organización; pérdidas financieras importantes, cobertura a nivel nacional y de forma prolongada; intervención regulatoria con sanciones por faltas muy graves: pérdida de clientes a gran escala.
Alto	Daño sobre la empresa es mayor, riesgo inusual o inaceptable en el sector, cobertura a nivel nacional, investigador de regulador y sanciones por falta grave; involucramiento de alta gerencia, gastos operativos de consideración; pérdidas financieras mayores.
Medio	El impacto sobre la entidad es directo y medio, se podría incurrir en gastos operativos controlados, existen sanciones por falta leve, se expone la imagen de la organización con un impacto medio.
Bajo	Riesgo aceptable en el sector, no hay daño de reputación, no hay sanciones legales, pero si observaciones por de parte de los reguladores, el impacto operacional o financiero es mínimo.
Muy Bajo	No hay impacto directo sobre la organización, no hay daño a la reputación, no existe sanciones legales ni impacto financiero u operacional; no es percibido por los clientes pero si por los colaboradores.

Fecha: _____ Firma del encuestador

Responsable	Activo	¿Cuál es el impacto estimado en la Institución?		Escala				
		Vulnerabilidad	Amenaza	Muy Alto	Alto	Medio	Bajo	Muy bajo
	Computadora de escritorio	Falta de cierre de sesión al momento de salir de la estación de trabajo	Manipulación de la información					

Tabla N°06: Ejemplo de Cuestionario N° 1
Elaboración Propia

Anexo A.11: Validez de Cuestionario N° 02

Validez de contenido del cuestionario sobre el impacto estimado en la institución según los activos de información en la contratación de Personal Docente en la DREP.

Estimado(a) Ingeniero/Maestro/Doctor:

Ing. Chunga Zapata Elmer Alfredo

Siendo conocedor de su trayectoria académica y profesional, me he tomado la libertad de elegirle como JUEZ EXPERTO para revisar el contenido del cuestionario que pretendo utilizar para determinar el impacto que hay en que cierta amenaza explote la vulnerabilidad.

A continuación presento una lista de afirmaciones (ítems) relacionadas a cada concepto teórico. Lo que se le solicita es marcar con una X el grado de pertenencia de cada ítem con su respectivo concepto, de acuerdo a su propia experiencia y visión profesional. No le pido que responda las preguntas de cada área, sino que indique si cada pregunta es apropiada o congruente con el concepto o variable que se pretende medir.

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido del presente cuestionario. De antemano agradezco su cooperación.

B. Información sobre el especialista

Sexo	: Varón (x) Mujer ( )
Edad	: 43 Años
Profesión o especialidad	: Ingeniero Informático
Años de experiencia laboral	: 13 años
No. ID. Colegio Profesional	: 90955

Elmer Alfredo Chunga Zapata
Ingeniero Informático
Reg. del Colegio de Ingenieros N° 90955

Anexo A.12: Guía de Observación Nº 04

Análisis de Riesgos de los activos de Información del proceso de Contratación de Personal Docente en la Dirección Regional de Educación basado en las directrices de la ISO/IEC 27005.

Guía de Observación Nº 04:

Objetivo: Verificar la existencia de procedimientos para evitar el acceso físico no autorizado.

Instrucciones: Escribir de forma clara, usar lapicero de color azul o negro, no se acepta el uso de corrector.

DATOS GENERALES:

INSTITUCIÓN: Dirección Regional de Educación- PIURA.

ÁREA: Centro de computo.

FECHA: ____/____/____

N°	Procedimientos	Existencia	
		Sí	No
1	Perímetro de seguridad definido.		
2	Barreras físicas, alarmas, etc.		
3	Personal de vigilancia.		
4	Identificación visible para el personal.		
5	Revisión y actualización de los derechos de acceso.		
6	Registro de visitas.		
	Número de Controles		

NOTAS:

_____
_____
_____
_____

Anexo B: Desarrollo de las etapas del análisis de riesgos

Anexo B.1: Identificación de los activos

Tipos de Activos	Activo de información	Responsable	Actividad	Descripción del Activo
Tecnología	Computadora de Escritorio	Técnico Administrativo. Tramite Documentario	Digitar Cargos por fecha y por motivo, previo descargo en el STD (sistema de tramite documentario)	Computadoras utilizadas por el personal para realizar labores como el importado de las bases de datos,etc.
		Técnico Administrativo. Dir. Gestión Institucional	Recepciona, verifica la existencia de plaza codificada por NEXUS, registra el nombre del Trabajador en el Libro de Control de Ejecución, visa y deriva a su Jefatura.	
	Cableado de Ethernet	Ingeniero Informatico del centro de computo	Se utiliza para tener conectividad con el Ministerio de Educación así como a internet.	Cable que interconectar incluyendo impresoras, discos externos, routers, escaners, switches y por supuesto las propias computadoras.

	Impresora	Utilizado por Técnico administrativo del área de Personal	Para imprimir Proyectos de resoluciones directorales	Herramientas utilizadas para imprimir en el área
	Fotocopiadora	Utilizado por Especialista administrativo de la Dir. Tramite Documentario.	Reproduce copias de distintos documentos para tener obtener cargos de estos documentos.	La fotocopia es el resultado de reproducir un documento, o parte de este, en una hoja de papel normal u otro tipo de material, como transparencias o filminas, opalina, etcétera.
APLICACIÓN	Licencia De Microsoft Windows XP	Ingeniero Informatico del centro de computo	Sistema Operativo actualmente instalado en las computadoras de escritorio en las oficinas de la DREP.	Licencia de Microsoft adquirida para ser distribuida en todas las computadoras de la DREP
	Licencia De Microsoft Office 2007	Ingeniero Informatico del centro de computo	Microsoft Office 2007 es actualmente instalado en las computadoras de escritorio en las oficinas de la DREP.	Licencia de Microsoft Office 2007 adquirida para ser distribuida en todas las computadoras de la DREP
	Red de la DREP	Ingeniero Informatico del centro de computo	La red en la DREP es tipo estrella, para la conectividad de internet entre las computadoras de escritorio para las oficinas que necesiten.	Red tipo estrella es la que maneja la DREP.

Sistema de información NEXUS	Técnico Administrativo de la Dirección de Gestión Institucional.	NEXUS es un Sistema para la Administración y Control de Plazas docentes, administrativos del sector educación.	En el sistema NEXUS se tiene información actualizada de las plazas vacantes de las instituciones educativas, según niveles y modalidades educativas y diferentes requerimientos que requiere el MINEDU y la DREP.
Sistema de Tramite Documentario	Técnico Administrativo. Tramite Documentario	Sistema Integrado de Tramite Documentario en la Dirección Regional de Educación e instancias de gestión Educativa.	Sistema para el registro de documentos, teniendo en cuenta el tipo de trámite, los números de folio, el origen, el asunto del documento y la programación de ruta o sea a que oficina o dependencia se deriva.
Servidores	Ingeniero Informatico del centro de computo	Con este servidor se conectara a las aplicaciones del sistema NEXUS, así como la base de datos de las plazas codificadas.	Es un programa informático que procesa una aplicación del lado del servidor, realizando conexiones bidireccionales y/o unidireccionales y síncronas o asíncronas con el cliente y generando o cediendo una respuesta en cualquier lenguaje o Aplicación del lado del cliente.

	Página Web De La DREP		Aplicación o portal donde se publican las plazas adjudicadas según el número de resoluciones directorales, es un medio donde los docentes pueden ver el reporte de aquellas plazas a las que se postuló.	Aplicación desarrollada por el ingeniero Informatico de la DREP para emitir informacion de todos los ámbitos de la gestión educativa que está desarrollando en la región Piura.
	Archivadores para los documentos de todas las Áreas que intervienen en la contratación de personal Docente	Secretaria	Se resguardan la documentación a presentar, como también libros de cargos donde se registran los cargos.	Los archivadores de se resguardan, los libros de cargo, resoluciones, copias de documentos, etc.
	Sello de transcripción	Técnico Administrativo. Tramite Documentario	Representación gráfica donde se resume la fecha de la emisión de la Resolución Direccional.	Es un sello que lo proporciona el técnico de la dirección de trámite documentario.
	UPS (sistema de alimentación)	Ingeniero Informatico del centro de computo	Es un dispositivo que maneja un sistema de alimentación ininterrumpida, para que los servidores de la DREP sigan trabajando por si hay algún desperfecto eléctrico.	Sistema de Alimentación Ininterrumpida es un conjunto de dispositivos estáticos (eléctricos y electrónicos) que aseguran el suministro sin interrupción de una energía eléctrica de calidad. Las UPS además de suministrar energía eléctrica ininterrumpida en caso de corte de red durante un cierto tiempo, protegen ante variaciones de tensión o perturbaciones, suministrando una energía "limpia y estable".

DATOS	Curriculum Vitae Documentado	Técnico Administrativo de Tramite Documentario	Documentación presentada para el registro y formalizar el vínculo contractual con el Servidor Civil.	Curriculum Vitae Documentado previament foliado y visado por la DREP para que tenga validación que es fiel copia a la original presentada y que es reconocida por la DREP.
	FUT (formulario único de trámite)			FUT (formato Único de Trámite) es la solicitud que debe nombrar la plaza a la postulada y a que UGEL pertenece.
	Cargo de documentación		Es la copia del documento presentado en la solicitud debidamente foliado.	En el cargo se emite la fecha y el número de folios que ha tenido la documentación presentada.
	Registro de documento al STD		Se registra la los folios, la fecha en la que se ha entregado y se envía al área de Personal para que siga el procedimiento para la contratación.	Este registro se tendrá en cuenta la fecha, asunto y que dependencia es enviada para el seguimiento del proceso.

	Número Resolución Directoral	Técnico administrativo del Área de Personal	Digitar número Resolución Directoral	Se emite un número de resolución Directoral para identificar el proceso que se está haciendo para responder a la solicitud del tramite
	Proyecto de Resolución Directoral	Técnico administrativo del Área de Personal	Es un documento que da con formalidad la respuesta a la solicitud demandada por el docente.	Es un documento formal que el director Regional de educación emite ante las solicitudes interpuestas por los docentes.
	Tipo de contrato	Técnico administrativo del Área de Personal	Dato que se toma en cuenta el encargado para saber el tipo de remuneración se tiene que atribuirle al docente.	El tipo de contrato se da según la plaza que se ha ganado en concurso según el nivel y la zona en donde se desarrolla el contrato.

	Libro de control de ejecución	Técnico administrativo del Área de Personal	se lleva el control la ejecución del contrato para el docente asignado.	Es un libro donde se tiene control la ejecución del contrato para el docente asignado.
	Libro de cargos de Asesoría Jurídica	Secretaria de Asesoría Jurídica	Es un libro donde se registran los copias con sello de cargo recibidas al despacho de asesoría jurídica	En este libro se encuentran registrados todos los documentos recepcionados, debidamente con la fecha y el código de donde ha sido antes enviado.
	Libro de cargos del Área de Personal	Secretaria Área de Personal	Es un libro donde se registran los copias con sello de cargo recibidas al despacho del Área de Personal	En este libro se encuentran registrados todos los documentos recepcionados, debidamente con la fecha y el código de donde ha sido antes enviado.
	Libro de cargos de Dirección de Oficina de Administración	Secretaria Oficina de Administración	Es un libro donde se registran los copias con sello de cargo recibidas al despacho de la Oficina de Administración	Este libro se encuentran registrados todos los documentos recepcionados, debidamente con la fecha y el código de donde ha sido antes enviado.

	Libro de cargos de Dirección Gestión Institucional	Secretaria Dirección Gestión Institucional	Es un libro donde se registran los copias con sello de cargo recibidas al despacho de Dirección de Gestión Institucional	Este libro se encuentra registrados todos los documentos recepcionados, debidamente con la fecha y el código de donde ha sido antes enviado.
	Libro de cargos de Dirección Regional de Educación	Secretaria Dirección Regional de Educación	Es un libro donde se registran los copias con sello de cargo recibidas al despacho de la dirección	Este libro se encuentra registrados todos los documentos recepcionados, debidamente con la fecha y el código de donde ha sido antes enviado.
	Copias del de la Resolución Directoral Regional	Secretaria Dirección Regional de Educación	Estas copias son backups para tener como constancia de la misma.	
	Registro de número correlativo del documento en trámite Documentario	Técnico Administrativo de Tramite Documentario	Se emite el número de correlativo según el asunto de la solicitud	
	Registro del cargo del documento en el Área de Personal	Secretaria Área de Personal	Se registra la fecha en la que se entregado el cargo en el libro de cargos	

	Registro del documento Proyecto RDR en Dirección de Administración	Secretaria Proyecto RDR en Dirección de Administración	El registro se da en el libro de cargos de la Dirección de administración.	
	Registro del documento en Dirección de Gestión Institucional	Secretaria en Dirección de Gestión Institucional	El registro se da en el libro de cargos de la Dirección de Gestión Institucional.	
	Base de datos de plazas codificadas	Técnico administrativo Gestión Institucional.	Importar la base de datos de las plazas codificadas donde se muestran a quienes están destinados y a que UGEL pertenece	Esta base de datos es proporcionado por el Ministerio de Educación
	Registro del datos del trabajador al sistema NEXUS	Técnico administrativo de la Dirección de Gestión Administrativa	Se registra los datos completos del docente que ha ganado cierta plaza	El registro se da mediante el sistema informatico NEXUS donde se registran las plazas asignándole los datos del docente al que pertenece.
	Registro del cargo del documento en Dirección de Asesoría Jurídica	secretaria	El registro se da en el libro de cargos de la Dirección de Asesoría Jurídica.	
	Registro del documento en Dirección de Regional	secretaria	El registro se da en el libro de cargos de la Alta Dirección.	

Red	Switch	Ingeniero Informatico del centro de computo	Proporciona conectividad con la red de la DREP para tener acceso a Internet	Los conmutadores se utilizan cuando se desea conectar múltiples tramos de una red, fusionándolos en una sola red. Al igual que los puentes, dado que funcionan como un filtro en la red y solo retransmiten la información hacia los tramos en los que hay el destinatario de la trama de red, mejoran el rendimiento y la seguridad de las redes de área local
	HUB		Proporciona conectividad con la red de la DREP para tener acceso a Internet	Concentrador de puertos de Ethernet, es el dispositivo que permite centralizar el cableado de una red de computadoras, para luego poder ampliarla.

Instalación	Router		Proporciona conectividad con la red de la DREP para tener acceso a Internet	Es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes
	Oficinas	Propietarios de las oficinas son todos los funcionarios que trabajan en la DREP.	Espacio establecido para las coordinaciones entre los funcionarios administrativos, solo para personal autorizado.	Instalación en donde se ejercen los deberes de los funcionarios que trabajan en la DREP.
	Vitrinas Informáticas	Propiedad del área de Personal en donde se publican las plazas adjudicadas	En las vitrinas se publican detalladamente los números de los Proyectos de Resolución Directoral para todo el personal docente contratado.	instalación en donde se publican las plazas adjudicadas

Personal	Técnico administrativo de Tramite Documentario
	Especialista Administrativo de Tramite Documentario
	Especialista Administrativo de Área de Personal
	Técnico administrativo de Área de Personal
	Secretaria de la Oficina de Administración
	Director de la Oficina de Administración
	Secretaria de la Oficina de la Dirección de Gestión Institucional
	Técnico administrativo de la Dirección de Gestión Institucional
	Director de la Dirección de Gestión Institucional
	Secretaria de la Dirección de la Asesoría Jurídica
	Director de la Dirección de la Asesoría Jurídica
	Secretaria de la Dirección Regional de Educación
	Director Regional de Educación
	Técnico administrativo del área de escalafón
	Técnico de administración de personal
	Técnico administrativo del área de remuneraciones.
	Técnico administrativo de Órgano de control Institucional
	Secretaria de Institución Educativa
	Interesado/Docente
	Autógrafa
	Ingeniero Encargado del soporte Técnico

Anexo B.2: Valoración de los activos

valor	Criticidad
0	No aplica
1	Baja
2	Baja
3	Baja
4	Medio
5	Medio
6	Medio
7	Alta
8	Alta
9	Alta

Tabla N°1. Valores según el nivel de criticidad.

Criterio	Valor	Descripción
Disponibilidad	0	No aplica / No es relevante
	1	Debe estar disponible al menos el 10% del tiempo
	2	Debe estar disponible al menos el 50% del tiempo
	3	Debe estar disponible siempre
Integridad	0	No aplica / No es relevante
	1	No es relevante los errores que tenga o la información faltante
	2	Tiene que estar correcto y completo al menos en un 50 %
	3	Tiene que estar correcto y completo en un 100%
Confidencialidad	0	No aplica / No es relevante
	1	Daños muy bajos, el incidente no transcendería del área afectada
	2	Seria relevantes, incidente implicaría a otras áreas
	3	Los daños serian catastróficos, la reputación y la imagen de la organización se verían comprometidas

Tabla N°2. Criterios de Valorización de activos.

En la siguiente tabla se muestra los activos clasificados según su tipología, evaluando la criticidad que tiene cada activo de informacion, teniendo en cuenta las dimensiones de la seguridad de información como son la Integridad, Disponibilidad y la confidencialidad teniendo en cuenta la tabla anterior donde se da como resultado el nivel de criticidad en el que se encuentra cada activos; solo teniendo en cuenta para el siguiente etapa a los activos que tengan un nivel de criticidad “ALTA”.

Tipos de Activos	Nombre de Activo	Dimensiones			T	Criticidad
		I	D	C		
Tecnología	Computadora de Escritorio de Tramite Documentario y Personal	3	3	3	9	ALTA
	cableado de Ethernet	3	3	2	8	ALTA
	teléfono	3	3	0	6	MEDIO
	impresora	3	2	0	5	MEDIO
	fotocopiadora	3	2	0	5	MEDIO
Aplicación	Licencia De Microsoft Windows XP	3	3	1	7	ALTA
	Licencia De Microsoft Office 2007	3	3	1	7	ALTA
	Red de la DREP	3	2	3	8	ALTA
	sistema de información NEXUS y STD	3	3	3	9	ALTA
	Servidores para el sistema Informatico NEXUS (plazas codificadas) y STD	3	3	3	9	ALTA
	Página Web De La DREP	2	3	2	7	ALTA
Equipamiento Auxiliar	archivadores para los documentos	2	1	2	5	MEDIO
	archivos de Asesoría Legal	2	1	2	5	MEDIO
	UPS (sistema de alimentación)	2	3	1	6	MEDIO
	Sello de transcripción	3	2	1	6	MEDIO
	archivos de gestión Institucional	2	1	2	5	MEDIO
	Archivos del Área de Personal	2	1	2	5	MEDIO
Datos	FUT (Formato Único de Tramite)	2	2	2	6	MEDIO
	Curriculum Vitae Documentado	2	2	2	6	MEDIO
	Proyecto de Resolución Directoral	3	3	3	9	ALTA
	Libro de control de ejecución	3	3	3	9	ALTA

	Libro de cargos de Asesoría Jurídica	3	3	3	9	ALTA
	Libro de cargos de tramite Documentario	3	3	3	9	ALTA
	Libro de cargos del Área de Personal	3	3	3	9	ALTA
	Libro de cargos de Dirección de Oficina de Administración	3	3	3	9	ALTA
	Libro de cargos de Dirección Gestión Institucional	3	3	3	9	ALTA
	Libro de cargos de Dirección Regional de Educación	3	3	3	9	ALTA
	Copias del de la Resolución Directoral Regional	3	0	3	6	MEDIO
	Registro del documento en trámite Documentario	3	2	1	6	MEDIO
	Registro del documento en el Área de Personal	3	2	1	6	MEDIO
	Registro del documento Proyecto RDR en Dirección de administración	3	2	1	6	MEDIO
	Registro del documento en Dirección de Gestión Institucional	3	2	1	6	MEDIO
	Base de datos de plazas codificadas	3	3	3	9	ALTA
	Registro del datos del trabajador al sistema NEXUS	3	2	1	6	MEDIO
	Registro del documento en Dirección de Asesoría Jurídica	3	2	1	6	MEDIO
	Registro del documento en Dirección de Regional	3	2	1	6	MEDIO
Personal	Técnico administrativo de Tramite Documentario	3	2	0	5	MEDIO
	Especialista Administrativo de Tramite Documentario	3	2	0	5	MEDIO
	Especialista Administrativo de Área de Personal	3	2	0	5	MEDIO
	Técnico administrativo de Área de Personal	3	2	0	5	MEDIO
	Secretaria de la Oficina de Administración	3	2	0	5	MEDIO
	Director de la Oficina de Administración	3	2	0	5	MEDIO
	Secretaria de la Oficina de la Dirección de Gestión Institucional	3	2	0	5	MEDIO
	Técnico administrativo de la Dirección de Gestión Institucional	3	2	0	5	MEDIO
	Director de la Dirección de Gestión Institucional	3	2	0	5	MEDIO
	Secretaria de la Dirección de la Asesoría Jurídica	3	2	0	5	MEDIO
	Director de la Dirección de la Asesoría Jurídica	3	2	0	5	MEDIO
	Secretaria de la Dirección Regional de Educación	3	2	0	5	MEDIO
	Director Regional de Educación	3	2	0	5	MEDIO
	Técnico administrativo del área de escalafón	3	2	0	5	MEDIO
	Técnico de administración de personal	3	2	0	5	MEDIO
	Técnico administrativo del área de remuneraciones.	3	2	0	5	MEDIO
	Técnico administrativo de Órgano de control Institucional	3	2	0	5	MEDIO
	Secretaria de Institución Educativa	3	2	0	5	MEDIO
	Interesado/Docente	3	2	0	5	MEDIO

	Autógrafa	3	2	0	5	MEDIO
	Encargado del soporte Técnico	3	2	0	5	MEDIO
Red	Switch	2	3	1	6	ALTA
	Router	2	3	2	7	ALTA
	HUB	2	3	1	6	ALTA
Instalación	Oficinas del centro de computo	2	3	3	8	ALTA
	Vitrinas Informáticas	1	1	0	2	BAJA

Anexo B.3: Matriz de Riesgos

Probabilidad de Afectación	Interpretación
Muy Alta	Es casi seguro que la amenaza afectará la vulnerabilidad.
Alta	Es probable que la amenaza afectará la vulnerabilidad.
Media	Es posible que la amenaza afectará la vulnerabilidad.
Baja	Es improbable que la amenaza afectará la vulnerabilidad
Muy Baja	Es impensable que la amenaza afectará la vulnerabilidad

Tabla N° 3. Descripción de los niveles de probabilidad de afección.

Impacto en la Organización	Interpretación
Muy Alto	Pérdida o daño catastrófico a la reputación de la organización; pérdidas financieras importantes, cobertura a nivel nacional y de forma prolongada; intervención regulatoria con sanciones por faltas muy graves: pérdida de clientes a gran escala.
Alto	Daño sobre la empresa es mayor, riesgo inusual o inaceptable en el sector, cobertura a nivel nacional, investigador de regulador y sanciones por falta grave; involucramiento de alta gerencia, gastos operativos de consideración; pérdidas financieras mayores.
Medio	El impacto sobre la entidad es directo y medio, se podría incurrir en gastos operativos controlados, existen sanciones por falta leve, se expone la imagen de la organización con un impacto medio.
Bajo	Riesgo aceptable en el sector, no hay daño de reputación, no hay sanciones legales, pero si observaciones por de parte de los reguladores, el impacto operacional o financiero es mínimo.
Muy Bajo	No hay impacto directo sobre la organización, no hay daño a la reputación, no existe sanciones legales ni impacto financiero u operacional; no es percibido por los clientes pero si por los colaboradores.

Tabla N°4. Descripción de los niveles de Impacto en la DREP

Anexo B.4: Matriz de Calor

Impacto en la Organización	Probabilidad de Afectación				
	Muy Baja	Baja	Media	Alta	Muy Alta
	relevante	Relevante	Alto	Critico	Critico
Alto	Relevante	Relevante	Alto	Alto	Critico
Medio	Moderado	Moderado	Relevante	Alto	Critico
Bajo	Bajo	Bajo	Bajo	Moderado	Relevante
Muy Bajo	Bajo	Bajo	Bajo	Bajo	Moderado

Tabla N°5. Matriz de Calor.

Anexo B.5: Nivel de Riesgos

Nivel de Riesgo	Políticas para tomar acciones
critico	Riesgo no aceptable
Alto	Riesgo no deseable
relevante	Riesgo Aceptable
Moderado	Riesgo Aceptable
Bajo	Riesgo Aceptable

Tabla N°6. Plan de tratamiento de Riesgos.

1Anexo B.6: Resultado de la Matriz de Riesgos

MATRIZ DE RIESGOS						
Id de Riesgo	**Activo**	**Vulnerabilidad**	**Amenaza**	**Probabilidad de que la amenaza explote la vulnerabilidad**	**Impacto estimado en la institución**	**Nivel de Riesgo**
R1	Computadora de Escritorio de Tramite Documentario y Personal	Falta de cierre de sesión al momento de salir de la estación de trabajo	Manipulación de información	ALTO	ALTO	**ALTO**
R2		Sensibilidad a la humedad, polvo y al calor	Polvo, corrosión, congelamiento	MEDIO	MUY ALTO	**ALTO**
R3		Susceptibilidad a variaciones en el voltaje	Perdida de suministro de energía	ALTO	MUY ALTO	**CRITICO**
R4		Sensibilidad de golpes o caídas	Destrucción de equipos o medios de comunicación	BAJO	MUY ALTO	**RELEVANTE**
R5		Falta de backups de información.	Robo de información o del mismo equipo	MUY BAJO	MUY ALTO	**CRITICO**
R6		Mala seguridad de contraseñas	Espionaje remoto	MEDIO	MUY ALTO	**ALTO**
R7	Licencia de Microosoft Windows XP/ 2007	Falta de mecanismos de autenticación e identificación de usuarios	Abuso forzado de derechos	BAJO	MUY ALTO	**RELEVANTE**

R8		Mala gestión Contraseñas	Abuso forzado de derechos	BAJO	MUY ALTO	**RELEVANTE**
R9		Servicios innecesarios para el usuario	Procesamiento ilegal de los datos	ALTO	MUY ALTO	**CRITICO**
R10		Falta de mecanismos de autenticación e identificación de usuarios	Abuso o forzado de derechos	BAJO	ALTO	**RELEVANTE**
R11		Mala gestión de contraseñas	Abuso o forzado de derechos	BAJO	ALTO	**RELEVANTE**
R12		Servicios innecesarios para el usuario	Procesamiento ilegal de los datos	ALTO	ALTO	**ALTO**
R13	Página web de la DREP	Falta de pruebas del software	Abuso de derechos	MEDIO	MEDIO	**RELEVANTE**
R14		Defectos en el funcionamiento del software	Abuso de derechos	ALTO	MEDIO	**ALTO**
R15		Interfaz de usuario complicada	Error en el uso del software	ALTO	MEDIO	**ALTO**
R16		Falta de documentación	Error en el uso del software	MEDIO	MEDIO	**RELEVANTE**
R17		Servicios innecesarios para el usuario	Procesamiento ilegal de los datos	ALTO	MEDIO	**ALTO**
R18	Cableado Ethernet	Trafico de información desprotegido	Escuchar información ilegalmente	MEDIO	ALTO	**ALTO**

R19		Cableado desprotegido	Falla en los equipos de comunicaciones	ALTO	ALTO	**ALTO**
R20		Arquitectura de red insegura	Espionaje remoto	BAJO	ALTO	**RELEVANTE**
R21		Gestión inadecuada de la red	Saturación de los sistemas de información	ALTO	ALTO	**ALTO**
R22	Red de la DREP	Falta de controles en el traspaso de información	Robo de documentos o de equipos tecnológicos	ALTO	ALTO	**ALTO**
R23		Falta de privilegios en los permisos	Manipulación de información	MUY ALTO	ALTO	**CRITICO**
R24		Mala seguridad de contraseñas	Manipulación de información	ALTO	ALTO	**ALTO**
R25		Gestión inadecuada de la red	Saturación de los sistemas de información	ALTO	ALTO	**ALTO**
R26		Conexiones de red desprotegidas	Uso no autorizado de los equipos de red	MEDIO	ALTO	**ALTO**
R27	Sistema de información NEXUS y STD	Defectos en el funcionamiento del software	Abuso de derechos	MEDIO	MUY ALTO	**ALTO**

R28		Falta de cierre de sesión al momento de salir de la estación de trabajo	Manipulación de información	ALTO	MUY ALTO	**CRITICO**
R29		Falta de un log de pistas de auditoria	Abuso de derechos	MEDIO	MUY ALTO	**ALTO**
R30		Pocos o nulos controles de acceso	Abuso de derechos	ALTO	MUY ALTO	**CRITICO**
R31		Interfaz de usuario complicada	Error en el uso del software	ALTO	MUY ALTO	**CRITICO**
R32		Falta de documentación	Error en el uso del software	MEDIO	MUY ALTO	**ALTO**
R33		Servicios innecesarios para el usuario	Procesamiento ilegal de los datos	ALTO	MUY ALTO	**CRITICO**
R34	Servidores para el sistema Informatico NEXUS y STD	Falta de una adecuada gestión de reemplazo o mantenimiento	Destrucción de equipos o medios de comunicación	BAJO	MUY ALTO	**RELEVANTE**
R35		Sensibilidad a la humedad, polvo y al calor	Polvo, corrosión, congelamiento	MEDIO	MUY ALTO	**ALTO**
R36		Sensibilidad a la radiación	Radiación	MUY BAJO	MUY ALTO	**RELEVANTE**

		electromagnética	electromagnética			
R37		Susceptibilidad a variaciones en el voltaje	Perdida de suministro de energía	MEDIO	MUY ALTO	**ALTO**
R38		Susceptibilidad a variaciones en la temperatura	Fenómenos meteorológicos	MUY BAJO	MUY ALTO	**RELEVANTE**
R39		Sensibilidad de golpes o caídas	Destrucción de equipos o medios de comunicación	ALTO	MUY ALTO	**CRITICO**
R40		Falta de controles para acceder al ambiente del servidor	Robo de documentos o de equipos tecnológicos	ALTO	MUY ALTO	**CRITICO**
R41	Registro de documento al STD	Falta de mecanismos de backup	Robo o pérdida de documentos	MUY ALTO	ALTO	**CRITICO**
R42		Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	BAJO	ALTO	**RELEVANTE**
R43		Pocos o nulos controles de acceso	Robo o manipulación del activo	MUY ALTO	ALTO	**CRITICO**
R44	Registro de Resolución Directoral	Falta de mecanismos de backup	Robo o pérdida de documentos	MUY ALTO	ALTO	**CRITICO**

R45		Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	BAJO	ALTO	**RELEVANTE**
R46		Pocos o nulos controles de acceso	Robo o manipulación del activo	MUY ALTO	ALTO	**CRITICO**
R47	Proyecto de Resolución Directoral	Falta de mecanismos de backup	Robo o pérdida de documentos	BAJO	MUY ALTO	**RELEVANTE**
R48		Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	MEDIO	MUY ALTO	**ALTO**
R49						
		Pocos o nulos controles de acceso	Robo o manipulación del activo	ALTO	MUY ALTO	**CRITICO**
R50	Tipo de Contrato	Falta de mecanismos de backup	Robo o pérdida de documentos	MUY ALTO	ALTO	**CRITICO**
R51		Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	BAJO	ALTO	**RELEVANTE**

R52	Libro de control de ejecución	Falta de mecanismos de backup	Robo o pérdida de documentos	ALTO	ALTO	**ALTO**
R53		Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	BAJO	ALTO	**RELEVANTE**
R54		Pocos o nulos controles de acceso	Robo o manipulación del activo	MUY ALTO	ALTO	**CRITICO**
R55		Sensibilidad a la humedad, polvo y al calor	Polvo, corrosión, congelamiento	ALTO	ALTO	**ALTO**
R56	Libro de cargos de Asesoría Jurídica	Falta de mecanismos de backup	Robo o pérdida de documentos	ALTO	ALTO	**ALTO**
R57		Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	BAJO	ALTO	**RELEVANTE**
R58		Pocos o nulos controles de acceso	Robo o manipulación del activo	MUY ALTO	ALTO	**CRITICO**
R59		Sensibilidad a la humedad,	Polvo, corrosión,	MEDIO	ALTO	**ALTO**

		polvo y al calor	congelamiento			
R60	Libro de cargos de tramite Documentario	Falta de mecanismos de backup	Robo o pérdida de documentos	ALTO	ALTO	**ALTO**
R61		Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	BAJO	ALTO	**RELEVANTE**
R62		Pocos o nulos controles de acceso	Robo o manipulación del activo	MUY ALTO	ALTO	**CRITICO**
R63		Sensibilidad a la humedad, polvo y al calor	Polvo, corrosión, congelamiento	MEDIO	ALTO	**ALTO**
R64	Libro de cargos del Área de Personal	Falta de mecanismos de backup	Robo o pérdida de documentos	ALTO	ALTO	**ALTO**
R65		Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	BAJO	ALTO	**RELEVANTE**
R66		Pocos o nulos controles de acceso	Robo o manipulación del activo	MUY ALTO	ALTO	**CRITICO**

R67		Sensibilidad a la humedad, polvo y al calor	Polvo, corrosión, congelamiento	MEDIO	ALTO	**ALTO**
R68	Libro de cargos de Dirección de Oficina de Administración	Falta de mecanismos de backup	Robo o pérdida de documentos	ALTO	ALTO	**ALTO**
R69		Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	BAJO	ALTO	**RELEVANTE**
R70		Pocos o nulos controles de acceso	Robo o manipulación del activo	MUY ALTO	ALTO	**CRITICO**
R71		Sensibilidad a la humedad, polvo y al calor	Polvo, corrosión, congelamiento	MEDIO	ALTO	**ALTO**
R72	Libro de cargos de Dirección Gestión Institucional	Falta de mecanismos de backup	Robo o pérdida de documentos	ALTO	ALTO	**ALTO**
R73		Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	BAJO	ALTO	**RELEVANTE**
R74						

		acceso	activo			
R75		Sensibilidad a la humedad, polvo y al calor	Polvo, corrosión, congelamiento	MEDIO	ALTO	**ALTO**
R76	Libro de cargos de Dirección Regional de Educación	Falta de mecanismos de backup	Robo o pérdida de documentos	ALTO	ALTO	**ALTO**
R77		Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	BAJO	ALTO	**RELEVANTE**
R78		Pocos o nulos controles de acceso	Robo o manipulación del activo	MUY ALTO	ALTO	**CRITICO**
R79		Sensibilidad a la humedad, polvo y al calor	Polvo, corrosión, congelamiento	MEDIO	ALTO	**ALTO**
R80	Base de datos de plazas codificadas	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	BAJO	ALTO	**RELEVANTE**

R81	Oficinas del centro de computo	Uso inadecuado o descuido del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios	ALTO	ALTO	ALTO
R82		Ubicación en un área susceptible de inundación	Inundación	ALTO	ALTO	ALTO
R83		Falta de protección Física de las puertas y ventanas de la edificación	Hurto de equipo	ALTO	ALTO	ALTO
R84	Personal Administrativo	Entrenamiento insuficiente en seguridad	Error en el uso	ALTO	ALTO	ALTO
R85		falta de conciencia acerca de la seguridad	Error en el uso	ALTO	ALTO	ALTO
R86		falta de mecanismos de monitoreo	Procesamiento Ilegal de los Datos	MUY ALTO	ALTO	CRITICO

R87		Falta de politicas para el uso correcto de los medios de telecomunicaciones y mensajeria	Uso no autorizado del equipo	MEDIO	ALTO	ALTO

Tabla N° 11: Matriz de Riesgos
Elaboración Propia.

Anexo B.7: Propuesta de controles

Estos son los controles que se proponen para el tratamiento de los riesgos identificados; especificando el control, su descripción según la NTP-ISO/IEC 17799, los riesgos que mitigara, adecuada a la realidad de la organización.

Objetivos Control	Categoría De Seguridad	Nombre De Control	Descripción	Riesgos a controlar	Adaptación A La DREP
Seguridad Física	Áreas seguras	*Controles de entrada Físicos*	Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que solo se permita acceso al personal autorizado.	R40, R81, R83	Se deberán proteger las áreas seguras de la DREP mediante controles de entrada apropiados para asegurar que solo se permita acceso al personal autorizado.
		Seguridad de Oficinas, habitaciones y medios.	Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.	R40, R81, R83	Se deberán diseñar y aplicar controles de seguridad físicos en las oficinas, habitaciones y medios.
	Seguridad del Equipo	*Ubicación y protección del equipo*	El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.	R2	Los equipos electrónicos críticos deberán estar ubicados de tal manera que ayudaran a reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.
		Servicios Públicos	El equipo debe estar protegido de fallas de energía y de otras interrupciones causadas por fallas en los servicios públicos.	R3, R37	Los equipos electrónicos críticos deberán estar protegidos de fallas de energía y de otras interrupciones causadas por fallas en los servicios públicos.
		Seguridad en el cableado	El cableado de la energía y las telecomunicaciones que llevan data o sostienen servicios de información deben ser protegidos de la intercepción o daño	R19	El cableado eléctrico y de las telecomunicaciones que llevan data o sostienen los servicios de información de la DREP deberán ser protegidos mediante tubos u otros controles
					Los equipos deberán pasar por

		Mantenimiento de equipo	El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.	R2, R3, R37, R14	mantenimiento 1 vez mensual para asegurar la continuidad de los sistemas y demás aplicativos que dan soporte a los procesos críticos
Gestión de las comunicaciones y operaciones.	Planeación y Aceptación del sistema	*Aceptación del sistema*	Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación	R14,R15	Los Altos Directivos de la DREP deberán asegurar que los requerimientos y criterios de aceptación de los sistemas nuevos estén claramente definidos, aceptados, documentados y probados. Los sistemas de información nuevos, las actualizaciones y las versiones nuevas deberán pasar a producción luego de obtener la aceptación formal.
	Protección contra software malicioso y control móvil	*Controles contra Software malicioso*	Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso.	R14,R15	La protección contra códigos maliciosos se deberá basar en la detección de códigos maliciosos dentro de los sistemas del Ministerio de Educación y la reparación del software, conciencia de seguridad, y los apropiados controles de acceso a los sistemas.
	Respaldo (back-up)	*Back-up respaldo de la información*	Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.	R41, R44, R47, R50, R52,R56,R60,R64,R68,R72,R76	La DREP deberá proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y crítica se pueda recuperar después de algún desastre o falla de medios.
	Gestión de seguridad de Redes	*Controles de red*	Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.	R18,R19, R20,R21, R25, R26	El área de Centro de Cómputo de la DREP deberá implementar controles para asegurar la seguridad de la información en las redes, y proteger los servicios conectados de accesos no-autorizados.
			Se deben establecer los	R42,R45, R48,	Se deberán establecer procedimientos para la manipulación, procesamiento,

	Gestión de medios	*Procedimiento de manejo de la información*	procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso.	R51, R53, R57, R61,R65,R69, R73, R77, R80	almacenamiento y comunicación de la información consistente con su clasificación
	Intercambio de Información	*Procedimientos y Políticas de información y software*	Se deben establecer política, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.	R42,R45, R48, R51, R53, R57, R61,R65,R69, R73, R77, R80	Se deberán establecer políticas, procedimientos y controles para proteger el intercambio de información que se dé con en el Ministerio de Educación a través de todos los tipos de medios de comunicación que se manejen (teléfonos, correo electrónico, etc.).
		Mensajes electrónicas	Se debe proteger adecuadamente los mensajes electrónicos.	No existen riesgos identificados	La institución deberá manejar distintas políticas y controles que le permitan manejar de manera segura el intercambio de información vía Email.
	Monitoreo	*Registro de auditoria*	Se deben producir registros de las actividades de auditoría, excepciones y eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.	R29	La DREP deberá producir logs de auditoría, excepciones y eventos de seguridad de información. Estos registros se deben mantener durante un período determinado para ayudar en investigaciones futuras y monitorear los sistemas y aplicativos que se necesiten
		Uso del sistema de monitoreo	Se deben establecer procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado de las actividades de monitoreo se debe revisar regularmente.	R29	La DREP deberá determinar el nivel de monitoreo requerido para los medios individuales mediante una evaluación del riesgo. La institución deberá cumplir con los requerimientos legales relevantes aplicables para sus actividades de monitoreo.
		Inscripción del	Debe existir un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a todos los	R9, R17, R30, R43, R46, R49, R54, R58,	La DREP deberá manejar un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a los

	Gestión de Acceso del Usuario	*Usuario*	sistemas y servicios de información.	R62,R66, R70, R74, R78	usuarios de todos los sistemas y servicios de información que la institución posea.
		Gestión de Privilegios	Se debe restringir y controlar la asignación y uso de los privilegios.	R9, R17, R33, R10	Los sistemas multi-usuario del Ministerio de Educación que requieren protección contra el acceso no autorizado deberán controlar la asignación de privilegios a través de un proceso de autorización formal.
		Gestión de la Clave del usuario	La asignación de claves se debe controlar a través de un proceso de gestión formal.	R6, R8, R11, R24	El área de Sistemas deberá proporcionar directrices para la gestión para las contraseñas de los distintos sistemas de información que se posean. Estas políticas pueden abarcar la generación, cambio y entrega de la contraseña.
	Control de Accesos al sistema Operativo	*Sistema de Gestión de claves*	Los sistemas de manejo de claves deben ser interactivos y deben asegurar la calidad de las claves.	R6, R8, R11, R24	El área de Centro de cómputo deberá proporcionar políticas para las contraseñas de sesiones de Windows de los colaboradores con acceso a una PC. Estas políticas pueden abarcar la generación, cambio y entrega de la contraseña.
	Responsabilidades del Usuario	*Uso de clave*	Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.	R6, R8, R11, R24	El área de centro de cómputo deberá proporcionar políticas para las contraseñas de los distintos sistemas de información que se posean. Estas políticas deberán seguir buenas prácticas de seguridad en la selección y uso de claves.
		Equipo de usuario desatendido	Se debe requerir que los usuarios se aseguren de dar la protección apropiada al equipo desatendido	R1, R28	Todos los usuarios del Ministerio de Educación deberán estar al tanto de los requerimientos de seguridad y los procedimientos para proteger su respectivo equipo desatendido, así como sus responsabilidades para implementar

Control de Accesos.					dicha protección
	Responsabilidades del Usuario	*Política de pantalla y escritorio limpio*	Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.	R1, R5	La políticas de escritorio limpio y pantalla limpia que la alta dirección proporcione deberá tomar en cuenta las clasificaciones de información, requerimientos legales y contractuales y los correspondientes riesgos y aspectos culturales de la organización
	Control de Acceso a Redes	*Políticas sobre el uso de servicios en red*	Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.	R26	Se deberá formular una política relacionada con el uso de las redes y los servicios de la red, de tal manera que los usuarios del DREP sólo deberán tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.
	Control de Acceso al sistema Operativo	*Identificación y autentificación del usuarios*	Todos los usuarios deben tener un identificador singular (ID de usuario) para su uso personal y exclusivo, se debe elegir una técnica de autenticación adecuada para verificar la identidad del usuario.	R5, R6	Todos los usuarios de los sistemas de la DREP deberán tener un identificador singular (ID de usuario) para su uso personal y exclusivo (incluyendo el personal de soporte técnico, operadores, administradores de redes, y administradores de bases de datos) para poder verificar la identidad de la persona que acceda a la PC.
		Uso de utilidades del sistema	Se debe restringir y controlar estrictamente el uso de los programas de utilidad que podrían superar al sistema y los controles de aplicación.	R9, R17, R33, R10	Se restringirá y controlará estrictamente el uso de los programas de utilidad que podrían ser capaces de superar los controles de Windows y de las aplicaciones a las cuales el usuario tiene acceso.
		Sesión inactiva	Las sesiones inactivas deben cerrarse después de un período de inactividad definido.	R1, R28	Las sesiones inactivas de los usuarios de Windows deberán cerrarse después de un período de inactividad definido por el área de Sistemas.

	Control de acceso a la aplicación de información	*Aislamiento del sistema sensible*	Los sistemas sensibles deben tener un ambiente de cómputo dedicado (aislado).	R35, R36, R37, R39	Los sistemas críticos deberán tener un ambiente de cómputo dedicado (aislado) respecto a los demás sistemas que la institución educativa maneje. Esta área seguirá otro lineamiento de seguridad (por su nivel de criticidad).
Adquisición, desarrollo y mantenimiento de los sistemas de información	Requerimiento de Seguridad de los sistemas.	*Análisis y especificaciones de los requerimientos de seguridad*	Los enunciados de los requerimientos comerciales para sistemas nuevos, o mejorar los sistemas existentes deben especificar los requerimientos de los controles de seguridad.	R30, R33	Los requerimientos de seguridad deberán ser integrados en las primeras etapas de los proyectos de sistemas de información. Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.

Tabla N° 12: Controles Propuestos

Anexo C: Proceso de Contratación de Personal Docente

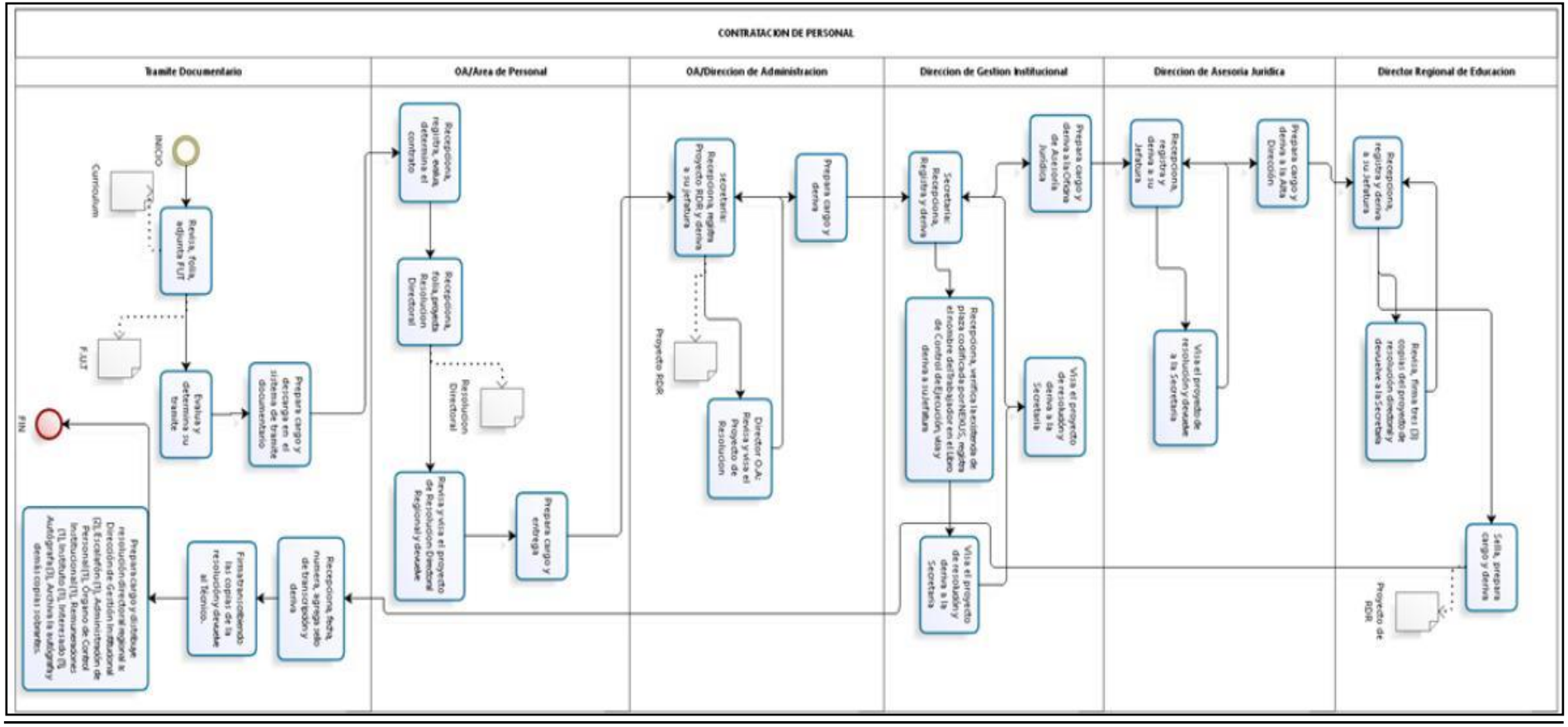


Figura N° 1: Diagrama BPM del proceso de contratación de personal docente.

Elaboración propia

MANUAL DE PROCEDIMIENTOS ADMINISTRATIVOS DE LA DIRECCIÓN REGIONAL DE PIURA

Unidad Orgánica Responsable: Administración
Área: Personal

Contrato de servidor civil: formalizar el vínculo contractual del servidor civil, con carácter temporal o accidental o según los términos del contrato y las disposiciones vigentes.

FINALIDAD

Formalizar el vínculo contractual del Servidor Civil, con carácter temporal o accidental según los términos del contrato y las disposiciones vigentes.

BASE LEGAL

- Ley del Presupuesto Público
- Ley N° 30057, Ley del Servicio Civil
- Ley Nº 27444, Ley del Procedimiento Administrativo General
- Decreto Supremo N° 040-2014-PCM, Reglamento de la Ley del Servicio Civil
- Ley Nº 29944 –Ley Reforma Magisterial
- Ley N° 29394, Ley de Institutos y Escuelas de Educación Superior
- Decreto Legislativo N° 276 – Ley de Bases de la Carrera Administrativa y de Remuneraciones del Sector Público, Art. 15º
- Decreto Supremo N° 004 –2013-D, Reglamento de la Ley de Reforma Magisterial.
- Decreto Supremo N° 011-2012-ED, Reglamento de la Ley General de Educación
- Decreto Supremo N° 004-2010-ED, Reglamento de la Ley de Institutos y Escuelas de Educación Superior
- Decreto Supremo N° 005-90-PCM, Reglamento del Decreto Legislativo Nº 276, Art. 28º, 39º y 40º
- Directiva sobre procedimientos para contratación emitidas por el Ministerio de Educación

REQUISITOS

- Solicitud FUT dirigido al Director Regional de Educación
- Currículo Vitae documentado y autenticado del postulante
- Disponibilidad presupuestal
- Haber aprobado el proceso de selección correspondiente

ACTIVIDADES

PASO	ACTIVIDAD	UNIDAD ORGÁNICA	RESPONSABLE
FASE 1		**INICIO**	
01	Recepciona File del Postulante, revisa, folia, adjunta hoja de trámite con número correlativo de registro o expediente, registra el documento presentado por el usuario y lo deriva al Especialista Administrativo.	DIR/Trámite Documentario	Técnico Administrativo
02	Evalúa, determina su trámite y devuelve al Técnico Administrativo.	DIR/Trámite Documentario	Especialista Administrativo
03	Prepara el cargo y entrega el documento al Área de Personal, previo descargo en el Sistema de Trámite Documentario	DIR/Trámite Documentario	Técnico Administrativo
FASE 2		**PROCESAMIENTO**	
04	Recepciona, registra, evalúa, determina el contrato y deriva al Técnico Administrativo.	OAIE/Personal	Especialista Administrativo
05	Recepciona, folia, proyecta Resolución Directoral y entrega al Especialista Administrativo	OAIE/Personal	Técnico Administrativo -
06	Revisa y visa el proyecto de Resolución Directoral Regional y devuelve.	OAIE/Personal	Especialista Administrativo
07	Prepara cargo y entrega a Secretaria	OAIE/Personal	Técnico Administrativo -
08	Recepciona, registra proyecto de RDR y deriva a su Jefatura	OAIE/Dirección	Secretaria
09	Revisa y visa el proyecto de resolución y devuelve a la Secretaria	OAIE/Dirección	Director de Oficina
10	Prepara cargo y deriva a la Oficina de Gestión Institucional	OAIE/Dirección	Secretaria
11	Recepciona, registra y deriva al Técnico Administrativo	Direc. Gestión Instituc.	Secretaria
12	Recepciona, verifica la existencia de plaza	Direc. Gestión Instituc.	Técnico Administrativo

	codificada por NEXUS, registra el nombre del Trabajador en el Libro de Control de Ejecución, visa y deriva a su Jefatura		
13	Visa el proyecto de resolución y deriva a la Secretaria	Direc. Gestión Instituc.	Director de Oficina
14	Prepara cargo y deriva a la Oficina de Asesoría Jurídica	Direc. Gestión Instit.	Secretaria
15	Recepciona, registra y deriva a su Jefatura	Direc. de Asesoría Jurídica	Secretaria – AJ
16	Visa el proyecto de resolución y devuelve a la Secretaria	Direc. de Asesoría Jurídica	Director de Oficina
17	Prepara cargo y deriva a la Alta Dirección	Direc. de Asesoría Jurídica	Secretaria – AJ
18	Recepciona, registra y deriva a su Jefatura	Dirección Regional	Secretaria
19	Revisa, firma tres (3) copias del proyecto de resolución directoral y devuelve a la Secretaria	Dirección Regional de Educación	Director Regional de Educación.
20	Sella, prepara cargo y deriva	Dirección Regional	Secretaria
21	Recepciona, fecha, numera, agrega sello de transcripción y deriva	DIR/Trámite Documentario	Técnico Administrativo
22	Firma transcribiendo las copias de la resolución y devuelve al Técnico.	DIR/Trámite Documentario	Especialista Administrativo
FASE 3	**TERMINO**		
23	Prepara cargo y distribuye resolución directoral regional a: Dirección de Gestión Institucional (2), Escalafón (1), Administración de Personal (1), Órgano de Control Institucional (1), Remuneraciones (1), Instituto (1), Interesado (1), Autógrafa (3), Archiva la autógrafa y demás copias sobrantes.	DIR/Trámite Documentario	Técnico Administrativo

Anexo D: Cuestionarios de la Investigación

Anexo D.1: cuestionario al centro de computo

EVALUACION DEL CENTRO DE CÓMPUTO DE LA DREP

-**Existe un buen sistema de conexión a tierra**

BUENO MEDIO MALO

-¿Qué porcentaje de importancia le da que exista un sistema de alimentación eléctrica de respaldo?

☐ **%**

-La DREP dispone de un área adecuada (cuarto frio) para activos tecnológicos.

BUENO MEDIO MALO

-¿Qué porcentaje de equipos de respaldo mantiene para servidores o equipos principales?

☐ **%**

-**La DREP cuenta con dispositivos físicos externos para resguardar.**

SI NO

-**¿La DREP cuenta con resguardo de activos de activos de información o auxiliares de forma lógica o física?**

SI NO

-¿La DREP cuenta con resguardo de activos de activos de información o auxiliares de forma externa?

SI NO

-¿Existen cámaras de vigilancias que tengas coberturas los activos tecnológicos?

SI NO

-¿La DREP posee un firewall de seguridad?

SI NO

-Con qué porcentaje de licenciamiento cuenta la DREP

☐ **%**

-Existe controles de en puertas a lugares de acceso restringido

SI NO

-Qué porcentaje de confianza tiene sobre el personal que opera los activos de TICS

☐ **%**

-¿Existen políticas de Tecnologías de información que hayan sido expuesta a los usuarios?

SI NO

Anexo D.2: Formato De Solicitud De Documentación.

"AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION "

Piura, 16 de Noviembre de 2015

Señor:

Ingeniero Luis Torres Preciado

Encargado de la Oficina de Centro de Computo

Presente.-

De mi consideración:

Por medio de la presente, es grato dirigirme a Usted a fin de saludarlo muy cordialmente, y comunicarle que como parte del desarrollo de mi tesis titulada: "Análisis De Riesgos De Los Activos De Información Del Proceso De Contratación De Personal Docente En La Dirección Regional De Educación Piura Basado En Las Directrices Del ISO/IEC 27005.". Se requiere la siguiente documentación:

- Organigrama interno.
- Manual de funciones y procedimientos administrativos de la DREP.
- Plan de seguridad de la información o similar.
- Manual de procesos y procedimientos del Centro de cómputo.
- Inventario de Hardware por tipo de equipo: Servidor, impresoras, equipos de comunicación.
- Inventario de Software por tipo de software: Sistema operativo, antivirus, software ofimático, utilitarios, otros.
- Plan de mantenimiento de Software y hardware o similar.
- Plan de contingencia o similar.
- Documentación técnica de los sistemas: Manuales, diagrama entidad relación, registro de incidentes, otros.

Por lo antes expuesto, solicito a usted me proporcione la información requerida. En caso no se cuente con la documentación o no pueda ser proporcionada, agradeceré se me indique por escrito como respuesta a la presente.

Seguro de contar con su apoyo, aprovecho la oportunidad para expresarle las muestras de mi especial consideración y estima.

Atentamente.

_____

Katia Chunga Ramírez

DNI N° 4621964

Anexo E: Informe de Evaluación de la Situación Actual

INFORME DE SITUAC

“Análisis de Riesgos de los activos de Información del proceso de Contratación de Personal Docente en la Dirección Regional de Educación basado en las directrices de la ISO/IEC 27005”.

Responsable:

Chunga Ramirez Katia

Periodo:

Del 30 Agosto al 30 de Noviembre de 2016

Emisión:

01 de Diciembre de 2016.

ÍNDICE

INTRODUCCIÓN

El presente informe corresponde a la Evaluación de la situación actual en la que se encuentran los activos de información del proceso de contratación de personal docente basado en las directrices del ISO/IEC 27005, llevada a cabo en coordinación con el centro de cómputo.

El contenido del presente informe se basa principalmente la evaluación de la situación actual, análisis de riesgos y emisión de conclusiones y recomendaciones con respecto a los puntos débiles o críticos detectados durante el estudio.

Durante la etapa de evaluación se revisó y analizó el resultado de los cuestionarios resueltos por al encargado del centro de cómputo y el personal de las demás áreas que intervienen este proceso. Asimismo se desarrolló siguiendo las directrices para realizar el análisis de riesgos:

g) Definición del alcance del modelo.
h) Identificación de activos.
i) Establecer las dimensiones de valoración de los activos.
j) Identificar Amenazas.
k) Determinar la probabilidad e impacto.
l) Identificar controles.

La evaluación se orienta a la determinación de la situación actual en cuanto a la seguridad de la información, con el fin de formular recomendaciones para mejorar estos mecanismos de control y/o proponer nuevos controles y/o procedimientos que reemplacen a los actualmente implementados. La implementación de mejoras y nuevos controles tiene el propósito minimizar la ocurrencia de riesgos futuros que pongan en peligro la seguridad de la información.

OBJETIVO GENERAL

- Analizar los riesgos evaluando los activos de información del proceso de Contratación de Personal Docente en la Dirección Regional de Educación de Piura.

OBJETIVOS ESPECIFICOS

- Identificar los activos de información del proceso de Contratación de Personal Docente en la DREP.
- Identificar vulnerabilidades y amenazas de los activos de información del proceso de Contratación de Personal Docente en la DREP.
- Proponer controles ante las amenazas identificadas de los activos de información del proceso de Contratación de Personal Docente en la DREP.

ALCANCE

Esta evaluación se realiza a los activos de información del proceso de contratación de personal docente en la Dirección Regional de Educación de Piura, y son los detallados a continuación:

1. **Definición del alcance:** El primer paso es definir el alcance para el análisis de riesgos. El alcance de esta evaluación son los activos que son integrantes en el proceso de Contratación de Personal Docente de la DREP.

2. **Identificación Activos de información:** se identificar dos tipos de activos: los primarios y los de soporte. Los primarios, según el estándar antes mencionado, “son los procesos e información más sensibles para la organización”. Los activos de soporte, “son los activos que dan el debido soporte a estos activos primarios”. Dentro de estas dos agrupaciones, se definieron siete distintos tipos específicos de activos: Dato, aplicación, personal, servicio, tecnología, instalación, equipamiento auxiliar.

3. **Dimensiones de Valoraciones:** Las dimensiones de valoración para los activos de información se tomaron en cuenta las tres propiedades bases del sistema de Gestión de seguridad de la informacion, la confidencialidad, la integridad y la disponibilidad de los activos según la ISO/IEC 27001 (2008).
4. **Identificar amenazas:** Según la ISO/IEC 27001 como parte del ciclo de vida de un SGSI, es necesario la identificación de las amenazas y vulnerabilidades a los que se encuentren expuestos los activos de información e identificar las debilidades en la seguridad de la información que puedan amenazar a los activos de información de la DREP.

5. **Determinar la probabilidad e impacto:** Para la Determinación de la Probabilidad e Impacto se debe llevar en conjunto con los propietarios de los activos de información, deben contestar las siguientes preguntas para determinar la probabilidad de ocurrencia de una amenaza: ¿Ya ha sucedido antes?, ¿pasa muy seguido? y ¿podría suceder?

6. **Identificar Controles:** Los controles son medios para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, practicas o estructuras organizacionales; para reducir, retener, evitar o transferir los riesgos y se debería definir un plan para tratamiento del riesgo.

METODOLOGIA

La evaluación se realizó teniendo en cuenta la ISO/IEC 27005, ya que ella nos brinda directrices para la gestión de riesgos de la seguridad de la informacion, dando soporte a los requerimientos de un SGSI. Sin embargo, esta norma no es de por si una metodología para la gestión de riesgos, aunque lo puede llegar a ser según el alcance del SGSI tenga o el contexto de la gestión de riesgos donde se aplique dicha norma.

DESARROLLO

La presente investigación se llevó a cabo entre los días de 30 junio del 2016 y 14 de Noviembre, como parte del análisis de riesgos de los activos de información en el proceso de contratación de personal docente en la DREP basado en las directrices del ISO/IEC 27005.

En la evaluación efectuada se ha empleado los siguientes procedimientos y técnicas:

- Cuestionario al encargado del Centro de computo de la DREP.
- Cuestionarios y entrevista con los responsables de cada área que interviene en el proceso de contratación.
- Evaluación a cada uno de los activos de información.
- Identificar que amenazas son más vulnerables los activos de información con un nivel de criticidad “Alta”.
- Cuestionar que tan probables y cuál sería el impacto que tendría la organización que estas amenazas se concreten.

Los datos recopilados fueron analizados y procesados a fin de permitir saber la situación actual en la que se encuentran expuestos los activos de información en el proceso de contratación de personal docente en la DREP para así poder brindar recomendaciones que ayuden minimizar el nivel de riesgo encontrado.

EQUIPO DE TRABAJO

El equipo de trabajo que realizado la evaluación estuvo conformado por 2 personas, que son el supervisor y el responsable de la evaluación. Siendo conformado por:

- Supervisor(a): MG. Quito Rodríguez Carmen Zulema.
- Responsable de la evaluación: Chunga Ramirez Katia.

AREAS EVALUADAS

- Trámite Documentario.
- Área de Personal.

- Dirección de Administración.
- Área de Gestión Institucional.
- Dirección de Asesoría Jurídica.
- Dirección Regional de Educación.

MARCO LEGAL

La evaluación se llevó a cabo en base al estándar internacional ISO/IEC 27005. Que tiene por título: Tecnología de la información- técnicas de seguridad - Gestión del riesgo en la seguridad de la información.

Esta norma suministra directrices para la Gestión del riesgo en la seguridad de la información.

Esta norma brinda soporte a los conceptos generales que se especifican en la norma ISO/IEC 27001 y está diseñada para facilitar la implementación satisfactoria de la seguridad de la información con base en el enfoque de gestión de riesgo.

El conocimiento de los conceptos, modelos, procesos y terminologías que se describen en la ISO/IEC 27001 y en la ISO/IEC 27002 es importante para la total comprensión de esta norma.

Esta norma se aplica a todos los tipo de organizaciones (por ejemplo empresas comerciales, agencias de gobierno, organizaciones sin ánimos de lucro) que pretenden gestionar los riesgos que podrían comprometer la seguridad de la información de la organización.

COMENTARIOS DE IMPORTANCIA

- El centro de cómputo de la DREP, por parte del encargado se dio como comentario que a este centro no se le asigne un plan de inversión ni se le da la importancia necesaria es por eso que existen fallas y no hay una disponibilidad al 100% en este centro de cómputo.

- Existen controles y procedimiento para el aseguramiento de la información, pero estos deben ser mejorados y documentados.

CONCLUSIONES

- Se debería desarrollar charlas y/o capacitaciones sobre la importancia de la seguridad de la información al personal que labora en la DIRESA, pues esto ayudaría en la gestión de la seguridad de la información.

- Se requiere de mayor grado control y compromiso por parte de los trabajadores respecto del uso de los implementos tecnológicos.

- Se debería elaborar e implementar un documento de políticas de seguridad.

- Se debería incluir o implementar un equipo de trabajo que realice labores de control interno para la gestión de la seguridad de la información, regulando la completa implementación y adaptación al estándar propuesto.

Anexo F: Documento de políticas de seguridad

DOCUMENTO
SEG

Responsable:

Chunga Ramirez Katia

Periodo:

Del 30 Agosto al 30 de Noviembre de 2016

Emisión:

01 de Diciembre de 2016.

POLÍTICA DE SEGURIDAD DE INFORMACIÓN

1. INTRODUCCION

La Dirección Regional de Educación de Piura es un órgano desconcentrado del Gobierno Regional de Piura. Claramente comprometida con el garantía de la seguridad de la información y con su personal docente, ha decidido incorporar, como parte de su estrategia institucional, la implementación de un sistema de gestión de la seguridad de la información o SGSI basado en los lineamientos presentados por la Norma Técnica Peruana ISO/IEC 27001:2014 dando cumplimiento la resolución Ministerial Nº 129-2014/DNB-INDECOPI.

2. OBJETIVOS DE LA POLITICA

Dar a conocer al personal administrativo de la Dirección Regional de Educación de Piura y a su ente rector que es el Ministerio de Educación, la importancia de una adecuada Gestión de Seguridad de información y todos los compromisos adquiridos para para proteger a un nivel aceptable por la organización, la información que posea, relacionada a los procesos administrativos que la DRE Piura este inmersa.

3. ALCANCE DE LA POLITICA

El cumplimiento de la presente política es de carácter obligatorio para todo el personal administrativo y para cualquier tercero, que tenga relación con el área de administración relacionado a los procesos incluidos dentro del alcance del SGSI.

4. ROLES Y RESPONSABILIDADES

La siguiente es una lista de roles y responsabilidades de la seguridad de la información al más alto nivel:

Alta Dirección

- Conocer y difundir la política de la seguridad de la información a todos los trabajadores de la organización.
- Estar comprometidos con la Gestión de la Seguridad de la Información.

Comité de Seguridad de Información:

- Comunicar la importancia de los objetivos de la seguridad de la información y la necesidad de mantener una mejora continua.
- Estar informados de las necesidades actuales de la organización y de los cambios dados en el proceso de contratación de personal docente.
- Facilitar y dar seguimiento a la asignación de recursos relacionados con el análisis de riesgos de los activos de información del proceso de contratación de personal docente.

Oficial de Seguridad de la Información:

- Diseñar, implementar, monitorear y mejorar el sistema de gestión de seguridad de la información en la empresa.
- Elaborar y ejecutar planes de capacitación para el personal involucrado en el proceso de contratación de personal docente de la DREP.
- Seleccionar y capacitar al personal adecuado para la auditoria interna del análisis de riesgos de los activos de información del proceso de contratación de personal docente.

Personal de la Organización:

- Conocer e identificar aquellos activos de información de los cuales son dueños.
- Asegurar que los activos de información que poseen son manejados y administrados correctamente.

- Reportar al oficial de seguridad de la información sobre cualquier vulnerabilidad detectada que afecta sus activos de información.

ANÁLISIS DE RIESGOS

1. INTRODUCCION

El presente documento describe los pasos necesarios para identificar y analizar los riesgos a los que se encuentra expuesta la organización, así como las acciones a realizar para el tratamiento de los mismos, en concordancia con lo propuesto por la ISO/IEC 27005:2008 referente a la gestión de riesgos en la seguridad de la información.

2. TERMINOS Y DEFINICIONES

Amenazas: según la ISO/IEC 27005:2008, es la causa potencial de un incidente de seguridad de la información no deseado, que puede resultar en un daño para la organización.

Apetito de riesgo: es el nivel máximo de riesgo que la organización está dispuesta a aceptar para el logro de sus metas.

Evaluación del riesgo: según la NTP ISO/IEC 31000:2009, es el proceso general de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

Impacto: según la ISO/IEC 27005:2008, son cambios adversos al nivel de los objetivos de la entidad logrados.

Probabilidad: posibilidad de que se materialice el riesgo, es decir, que se produzca un ataque exitoso de la amenaza, tomando en cuenta la vulnerabilidad y los controles existentes.

Riesgo: es la combinación de la probabilidad del ataque exitoso de la amenaza, y las consecuencias que acarrea dicho ataque (impacto).

Vulnerabilidad: es la debilidad de un activo o grupo de activos o controles, que puedan ser explotados por una o varias amenazas de acuerdo a su ubicación. Una vulnerabilidad en sí misma no causa daños.

3. PERSONAS AUTORIZADAS Y RESPONSABLES

La ejecución de lo indicado en este documento se encuentra a cargo del Oficial de Seguridad de la información, el comité de seguridad de la información y de cualquier persona autorizada por el centro de cómputo de la DRE Piura.

4. EVALUACION DE RIESGOS

4.1. Identificación de Amenazas y vulnerabilidades

Como parte del ciclo de vida del sistema de gestión de seguridad de la información, es necesario realizar la identificación de las amenazas y vulnerabilidades a los que se encuentran expuestos los activos de información e identificar las debilidades en la seguridad de la información que puedan amenazar a los activos de información de la entidad.

El oficial de seguridad de la información, deberá llenar el formato del anexo – Matriz de Riesgos", con la información obtenida tras entrevistar a los dueños de los activos según lo descrito en los siguientes pasos:

4.1.1. Identificación de Amenazas

Una amenaza tiene el potencial de dañar activos como sistemas, procesos o información, por ello, es muy importante

identificar cuáles son las amenazas principales a los que los activos de información están expuestos.

El oficial de seguridad de la información, junto con un personal debidamente capacitado, deberá realizar entrevistas a los dueños de los activos con la intención de identificar las amenazas ubicadas en el anexo – “lista de ejemplos de vulnerabilidades y amenazas” obtenido del “anexo D” de la ISO/IEC 27005:2008.

4.1.2. Identificación de vulnerabilidades

Las vulnerabilidades por si mismas no pueden ocasionar daños en los activos de información ya que necesitan alguna amenaza que las exploten; sin embargo, es necesario que sean debidamente identificadas en caso suceda algún cambio que implique la aparición de nuevas amenazas.

El oficial de seguridad de la información, junto con una persona debidamente capacitado, debe realizar entrevistas a los dueños de los procesos de identificación de estas vulnerabilidades, para ello podrá hacer uso de una “lista de ejemplos de vulnerabilidades y amenazas” obtenidas del anexo D de la ISO/IEC 27005:2008, el cual servirá como guía para esta labor.

4.2. Identificación y evaluación de Riesgos

Con ayuda de las amenazas y vulnerabilidades se podrá identificar fácilmente cuales son los riesgos que amenazan la información y podrá tomar medidas que ayuden a protegerla.

4.2.1. Identificación de Riesgos

El riesgo se definirá como la probabilidad que una amenaza explote una vulnerabilidad de un acto activo haciéndole perder alguna propiedad relacionada a la seguridad de la información (confidencialidad, integridad, disponibilidad.)

Una vez identificado el riesgo deberá ser ingresado en el anexo – “Matriz de riesgos”

4.2.2. Determinación de Probabilidades e Impacto

El oficial de seguridad de la información en conjunto con los dueños de los activos de información, deben contestar las siguientes preguntas para determinar la probabilidad de ocurrencia de una amenaza:

¿Ya ha sucedido antes?, ¿pasa muy seguido? y ¿podría suceder?

Para realizar esta valoración se recomienda revisar la siguiente tabla de lista de probabilidades.

Probabilidad de Afectación	Interpretación
Muy Alta	Es casi seguro que la amenaza afectará la vulnerabilidad.
Alta	Es probable que la amenaza afectará la vulnerabilidad.
Media	Es posible que la amenaza afectará la vulnerabilidad.
Baja	Es improbable que la amenaza afectará la vulnerabilidad
Muy Baja	Es impensable que la amenaza afectará la vulnerabilidad

De igual forma, deben determinar cuál es el impacto que tendría a la materialización de la amenaza considerando la vulnerabilidad y los controles existentes.

Para realizar esta valoración se recomienda revisar la siguiente tabla de lista de impactos:

Impacto en la Organización	Interpretación
Muy Alto	Pérdida o daño catastrófico a la reputación de la organización; pérdidas financieras importantes, cobertura a nivel regional y de forma prolongada; intervención regulatoria con sanciones por faltas muy graves: pérdida de clientes a gran escala.
Alto	Daño sobre la empresa es mayor, riesgo inusual o inaceptable en el sector, cobertura a nivel regional, investigador de regulador y sanciones por falta grave; involucramiento de alta gerencia, gastos operativos de consideración; pérdidas financieras mayores.
Medio	El impacto sobre la entidad es directo y medio, se podría incurrir en gastos operativos controlados, existen sanciones por falta leve, se expone la imagen de la organización con un impacto medio.
Bajo	Riesgo aceptable en el sector, no hay daño de reputación, no hay sanciones legales, pero si observaciones por de parte de los reguladores, el impacto operacional o financiero es mínimo.
Muy Bajo	No hay impacto directo sobre la organización, no hay daño a la reputación, no existe sanciones legales ni impacto financiero u operacional; no es percibido por los clientes pero si por los colaboradores.

4.2.3. Evaluación de nivel y valor del Riesgo

El nivel de los riesgos se obtendrá de la multiplicación de la probabilidad y el impacto previamente definido por los dueños

de los procesos lo cual permitirá ubicar al riesgo en uno de las siguientes celdas.

Impacto en la Organización	Probabilidad de Afectación				
	Muy Baja	**Baja**	**Media**	**Alta**	**Muy Alta**
Muy Alto	relevante	Relevante	to	Critico	Critico
Alto	Relevante	Relevante	to	to	Critico
Medio	Moderado	Moderado	Relevante		Critico
Bajo	Bajo	Bajo	Bajo		Relevante
Muy Bajo	Bajo	Bajo	Bajo		Moderado

Moderado

Bajo

4.2.4. Apetito del Riesgo

El comité de seguridad de la información es el responsable de aprobar el apetito del riesgo de la organización, en tal sentido, se ha definido:

- Riesgos Bajo - Moderado - Relevante: riesgos inferiores, deben ser tratados con los procedimientos de rutina ya definidos en la organización. Es hasta este punto en el cual se define el apetito del riesgo de la DRE Piura, es decir, aquellos riesgos que no se encuentren en esta zona deberán ser tratados para minimizar su valor.
- Riesgos Altos: Riesgos que deben ser tratados con procedimientos especiales con la ayuda de la implementación de algunos controles de seguridad, la alta dirección debe ser consciente de la existencia y tratamiento de estos riesgos.

- Riesgos Críticos: Riesgos que deben ser tratados de manera inmediata y con alta prioridad debido a lo que podría suceder si se materializa el riesgo, la alta dirección debe ser consciente de la existencia y tratamiento de estos riesgos.

4.2.5. Tratamiento del Riesgo

El oficial de seguridad de la información debe actualizar el Anexo – Matriz de riesgos" con los datos hallados en los pasos anteriores, una vez realizado esto deberá identificar quien o quienes son los responsables del tratamiento de los riesgos y evaluar las políticas para tomar acciones más apropiadas teniendo en cuenta el siguiente cuadro:

Nivel de Riesgo	Políticas para tomar acciones
critico	Riesgo no aceptable
Alto	Riesgo no deseable
relevante	Riesgo Aceptable
Moderado	Riesgo Aceptable
Bajo	Riesgo Aceptable

4.2.6. Controles

Una vez identificados y evaluados los riesgos cada uno de los riesgos que amenazan a los activos claves de la organización, el oficial de seguridad de la información, con la ayuda del ISO/IEC 27002, deberá identificar que controles ha de implementar para reducir el impacto o la probabilidad de los mismos hasta llevarlos a un nivel aceptable e introducir esta información dentro de la matriz de riesgo, a fin de mantener un registro de estos datos.

Los controles que se han seleccionado para el tratamiento de los riesgos son los que se detallan en el estándar ISO 27002, el cual contiene una lista bastante completa de objetivos de control y controles comúnmente relevantes para las organizaciones en general. Cabe resaltar que dichos controles siguen lineamientos generales, en la Declaración de la Aplicabilidad se mostrarán los controles adaptados a la realidad organizacional del instituto educativo estudiado.

Para empezar se definió controles respecto a las políticas de seguridad que la institución busca establecer para alcanzar el nivel de seguridad deseado. Cabe resaltar que todos estos controles o políticas contribuyen a la mitigación de todos los riesgos identificados y, en su mayoría, deberán ser desarrollados y promovidos por la Alta Gerencia de la entidad educativa.
Estos controles y políticas de seguridad son los siguientes:

Objetivos Control	Categoría de Seguridad	Nombre Control	Descripción
Política de seguridad	Política de seguridad de información	Documentar política de seguridad de información	La alta Dirección debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.
Revisión de la política de seguridad de la información		La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.	
Organización de la seguridad de la información	Organización interna	Compromiso de la gerencia con la seguridad de la información	La alta gerencia de debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.
Coordinación de la seguridad de información		Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.	
Asignación de responsabilidades de la seguridad de la información		Se deben definir claramente las responsabilidades de la seguridad de la información.	
Proceso de autorización para los medios de procesamiento de información		Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información.	
Acuerdos de confidencialidad		Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información.	
Gestión de activos	Responsabilidad por los activos	Inventarios de activos	Todos los activos deben estar claramente identificados y se debe

Objetivos Control	Categoría de Seguridad	Nombre Control	Descripción
Uso aceptable de los activos		Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.	
Clasificación de la información	Lineamientos de clasificación	La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.	
Etiquetado y manejo de la información		Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.	
Gestión de incidentes en la seguridad de la información	Reporte de eventos y debilidades en la seguridad de la información	Reporte de eventos en la seguridad de la información	Los eventos de seguridad de la información deben reportarse a través de los canales gerenciales apropiados lo más rápidamente posible.
Reporte de debilidades en la seguridad		Se debe requerir que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los sistemas o servicios.	
Gestión de incidentes y mejoras en la seguridad de la información	Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.	
Aprendizaje de los incidentes en la seguridad de la información		Deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.	
Recolección de evidencia		Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (sea civil o criminal), se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia	

		establecidas en la(s) jurisdicción(es) relevantes.	
Cumplimiento	Cumplimiento con requerimientos legales	Protección los registros organizacionales	Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.
Protección de data y privacidad de información personal		Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.	

Objetivos Control	Categoría de Seguridad	Nombre Control	Descripción
Prevención de mal uso de medios de procesamiento de información		Se debe desanimar a los usuarios de utilizar los medios de procesamiento de la información para propósitos no-autorizados.	
Gestión de las comunicaciones y operaciones	Procedimientos y responsabilidades operacionales	Procedimientos de operación documentados	Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.
Control de acceso	Gestión del acceso del usuario	Revisión de los derechos de acceso del usuario	La alta gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.
Adquisición, desarrollo y mantenimiento de los sistemas de información	Seguridad en los procesos de desarrollo y soporte	Desarrollo de outsource software	El desarrollo de software que ha sido outsourced debe ser supervisado y monitoreado por la organización.

Tabla N° 13: Políticas de Seguridad

Elaboración Propia

Anexo G: **DECLARACIÓN DE AUTORIA**

Yo, Katia Chunga Ramírez, estudiante de la Escuela profesional de Ingeniería de sistemas de la Universidad César vallejo, filial Piura; declaro que el trabajo académico título “Análisis de Riesgos de los activos de Información del proceso de Contratación de Personal Docente en la Dirección Regional de Educación basada en las directrices de la ISO/IEC 27005” presentada, en 139 folios para la obtención del título profesional de Ingeniero de Sistemas es de mi autoría.

Por tanto declaro lo siguiente:

- He mencionado todas las fuentes empleadas en el presente trabajo de investigación, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes, de acuerdo a lo establecido por las normas de elaboración de trabajos académicos.
- No he utilizado ninguna otra fuente distinta de aquellas expresamente señaladas en este trabajo.
- Este trabajo de investigación no ha sido previamente presentado completa ni parcialmente para la obtención de otro grado académico o título profesional.
- Soy consciente de que mi trabajo pueda ser revisado electrónicamente en búsqueda de plagios.
- De encontrar uso de material intelectual ajeno sin debido reconocimiento de su fuente o autor, me someto a las sanciones que determinan el procedimiento disciplinario.

Piura, 01 de Diciembre de 2017

Chunga Ramírez Katia

DNI 46219640